XOPERO
Backup&Recovery

CYBERBEZPIECZEŃSTWO

Trendy 2021

RAPORT

Wstęp 3

ROZDZIAŁ 1

Cyber Threats

Jakich zagrożeń możemy spodziewać się w nadchodzących miesiącach? 6

ROZDZIAŁ 2

Internet of Things

Urządzenia IoT to potencjalnie atrakcyjny wektor ataku. Czy jesteśmy gotowi na batalię z przestępcami? 23

ROZDZIAŁ 3

Cloud Computing

Trend multi-cloud oraz przybierająca na sile migracja do chmury - od cloud'a nie ma już odwrotu 30

ROZDZIAŁ 4

Machine Learning

Jako rolę odegra AI w projektowaniu nowej klasy rozwiązań dla specjalistów od cyberbezpieczeństwa? 42

ROZDZIAŁ 5

Backup i DR

Cloud backup, multi-cloud, cloud-native - w jakim jeszcze kierunku rozwija się obecnie rynek backupu? 51

ROZDZIAŁ 6

Security Gaps

Brak wykwalifikowanych specjalistów od cyberbezpieczeństwa - czy to problem, czy już katastrofa? 61

Podsumowanie 74

Drodzy czytelnicy,

witam w trzeciej edycji raportu Cyberbezpieczeństwo: Trendy 2021. Za nami trudny rok, którego wbrew badaniom, analizie dziesiątek dokumentów i analiz branżowych nie mogliśmy się spodziewać i przewidzieć. Rok, który uświadomił nam wszystkim jak wiele czynników naszego życia uzależnionych jest od nowych technologii. Odczuwalne stało się to zwłaszcza w momencie masowego przechodzenia na model pracy zdalnej przez organizacje. Szacuje się, że pandemia przyspieszyła rozwój tych praktyk o 5-10 lat. Firmy, które na co dzień nie stosowały takiego modelu, zostały zmuszone do szybkiego wdrożenia nowych mechanizmów, technologii i systemów zabezpieczeń. Od lat alarmujemy o niedostatecznym poziomie bezpieczeństwa IT w wielu firmach, które obnażyła właśnie praca zdalna. Niczym mantrę powtarzamy jedno z najbardziej powszechnych twierdzeń branżowych, że to człowiek stanowi największe zagrożenie dla całego systemu bezpieczeństwa. To właśnie w celu edukowania rynku, uświadamiania o tych problemach i zwiększania poziomu świadomości wśród kadry managerskiej i specjalistów IT tworzymy takie publikacje jak ten raport.

Paradoksalnie, cyberprzestępcy szybciej adaptują się do zmian i trendów rynkowych niż przedsiębiorstwa, a co za tym idzie, arsenał zagrożeń zmienia się w zatrważającym tempie. Dlatego też w ciągu całego roku staramy się monitorować i informować naszych użytkowników i klientów o aktualnych atakach, lukach i podatnościach oraz sposobach na zabezpieczenie danych w biznesie. W tym celu powstało Centrum Bezpieczeństwa Xopero, czyli przegląd najważniejszych newsów ze świata cyberbezpieczeństwa w formie cotygodniowego newslettera, którego skrótów nie sposób nie zamieścić w tym dokumencie.

Raport jest efektem pracy kilku specjalistów z Xopero Software, własnych badań ankietowych, analiz dziesiątek dokumentów branżowych, setek publikacji oraz indywidualnych obserwacji rynku. Do udziału w raporcie po raz kolejny zaprosiliśmy ekspertów z różnych firm działających w branży security i nowych technologii, po to, aby dołożyli swój punkt widzenia oraz dostarczyli praktycznych rad czytelnikom raportu. Dziękujemy każdemu specjaliście, który miał swój wkład w stworzenie tej publikacji.

Wierzymy, że merytoryczny charakter tego dokumentu, ilość włożonej w niego pracy, poświęconego czasu i pasji, pozwoli Państwu zwiększyć świadomość o bezpieczeństwie danych, zachęci do obserwowania najnowszych kierunków w branży i wreszcie, pozwoli Wam lepiej zabezpieczać swoje dane biznesowe.

Zapraszam do lektury.

Łukasz Jesis

CEO, Xopero Software

Wstęp

Podsumowując rok 2020 nie sposób nie wspomnieć kilku najważniejszych zdarzeń, które nie tylko odcisnęły piętno na całej branży cyberbezpieczeństwa, ale które mocno wpłyną na analizowane w ramach raportu trendy. Pierwszym z nich jest oczywiście wybuch pandemii, który wpłynął na kilka aspektów cyberbezpieczeństwa.

Po pierwsze - wymusił na firmach masowe przechodzenie na model pracy zdalnej, a tym samym obnażył ich nieprzygotowanie na ten nowoczesny system zatrudnienia. Okazało się, że przestarzały sprzęt, nie aktualizowane technologie czy brak rozwiązań typu SaaS utrudniały firmom sprawną organizację “home office”. Przed ogromnym wyzwaniem stanęli specjaliści ds. bezpieczeństwa i IT, którzy na gwałt musieli zorganizować pracownikom odpowiedni sprzęt, dostęp do zasobów firmy, sposób ewidencji czasu pracy czy bezpieczne metody uwierzytelniania pracowników zdalnych .

Po drugie, pandemia w sposób niewyobrażalny zwiększyła skalę zagrożeń. Poziom dezinformacji i strachu spowodował, że przestępcy nie musieli nawet silić się na kreatywność. Każda, nawet najbardziej oczywista kampania malspam zbierała żniwo. W początkowej fazie rozprzestrzeniania się wirusa dziennie powstawało kilkadziesiąt tysięcy fałszywych domen związanych z COVID-19! Mogliśmy więc mówić o korona-przestępczości w skali przemysłowej.

Jeżeli mowa o zagrożeniach, to zdecydowanie jednym z poważniejszych wciąż pozostaje ransomware, któremu poświęciliśmy sporą część raportu. 2020 rok spopularyzował nową technikę podwójnego wymuszenia (double-extortion) - czyli szantażowania ofiar nie tylko utratą zaszyfrowanych danych, ale również ich upublicznieniem. O ile na początku roku istniały zaledwie dwie strony do publikowania skradzionych informacji, na koniec było ich już siedemnaście. Autorzy ransomware zaczęli nawet formować kartel i wymieniać się technikami, praktykami i informacjami. To zdarzenie z pewnością wpłynie na krajobraz zagrożeń. Łatwa dostępność takich narzędzi na czarnym rynku, dostęp do technik i wiedzy wzbudzi zainteresowanie i aktywność początkujących cyberprzestępców.

O tym, jak ogromna jest skala cyberzagrożeń świadczą liczby. Oto kilka z nich:

- $ 3,86M - łączny średni koszt naruszenia ochrony danych w ujęciu globalnym (IBM)
- $150 - średnia cena jednego rekordu umożliwiającego identyfikację ofiary (IBM)
- $20B - szacowana wartość globalnych szkód spowodowanych przez ransomware w 2021 r.
- $15M - rekordowa wartość okupu zażądana przez cyberprzestępców w 2020 r.
- Co 11 sekund - z taką częstotliwością będzie uderzał ransomware

Na szczęście wraz z rozwojem zagrożeń, idzie poprawa skuteczności rozwiązań do zabezpieczania danych i branży bezpieczeństwa IT ogółem. Antywirusy i produkty anty-malware wykorzystują sztuczną inteligencję i uczenie maszynowe do jeszcze lepszej detekcji zagrożeń. Producenci rozwiązań do backupu danych śledząc trendy rynkowe, pogłębiają swoje oferty (cloud-native backup, cloud backup,

multi-cloud). Uwzględniając model pracy zdalnej umożliwiają także zabezpieczenie systemów i usług w chmurze (np. Microsoft 365 czy G Suite), oraz łatwą migrację całych infrastruktur między chmurami. Nacisk kładą na disaster recovery, a więc odtwarzanie awaryjne, które zabezpiecza ciągłość w realizowaniu procesów biznesowych zapewniając szybki dostęp do krytycznych usług i systemów.

Rośnie również wykorzystanie chmury - ponad 50% firm twierdzi, że w najbliższym czasie będzie ono wyższe, niż planowano. Przyczyną są doświadczenia związane z pracą zdalną i koniecznością zapewnienia dostępności zasobów firmowych. Już dziś firmy przeznaczają na chmurę ⅓ swoich inwestycji w IT. Niezaprzeczalnym trendem w 2021 roku będzie rozwój praktyki multicloud czy upowszechnianie się rozwiązań typu cloud-native security.

Wyzwaniem jest również stworzenie bezpiecznego Internetu Rzeczy, na który składa się już 80 miliardów połączonych ze sobą urządzeń. Szybki wzrost tego rynku, mało bezpieczny proces ich wdrożenia, brak stosownych aktualizacji czyni IoT szczególnie podatnym na ataki. Dodając do tego fakt, że do 2024 roku 35% całkowitego mobilnego ruchu danych będzie przenoszonych za pośrednictwem sieci 5G musimy już dziś nauczyć się zabezpieczać inteligentne urządzenia.

Co z najsłabszym ogniwem systemu cyberbezpieczeństwa, jakim wciąż pozostaje człowiek? Odpowiedzią jest cyberedukacja. O tym, jak wyglądają kompetencje zespołów security, w jaki sposób można je podnosić oraz czego oczekują sami zainteresowani, piszemy w rozdziale Security Gaps. Pamiętajmy jednak, że ten temat dotyczy każdego z nas. Najbardziej skuteczne i zaawansowane rozwiązania z zakresu bezpieczeństwa IT nie zdadzą się na nic, jeżeli my jako użytkownicy, pracownicy, managerowie i przedsiębiorcy nie nauczymy się bezpiecznego korzystania z Internetu. Właśnie w tym celu powstała niniejsza publikacja.

Cyber Threats
Przewidzieć nieprzewidywalne

Rok 2020 był unikatowy pod wieloma względami - nie sposób się z tym nie zgodzić. Już od dłuższego czasu obserwowaliśmy trend zwiększonej aktywności cyberprzestępców oraz ewolucji ich metod. Pandemia Covid-19 dołożyła nowy arsenał zagrożeń. Obawa przed nieznanym, masowe przechodzenie w tryb pracy zdalnej oraz wynikający z wybuchu pandemii poziom dezinformacji natychmiast pobudził kreatywność przestępców i spowodował wzrost ilości zagrożeń na niewyobrażalną dotychczas skalę. Operatorzy ransomware, którzy tuż po wybuchu pandemii ogłosili zaprzestanie ataków na placówki medyczne, bardzo szybko złamali swoją obietnicę. Zdając sobie sprawę z powagi sytuacji, kilka tygodni później dokonali pierwszych ataków na szpitale i instytuty badawcze. I tak też ransomware pozostał jednym z najgroźniejszych zagrożeń dla biznesu, co prawdopodobnie nie zmieni się również w nadchodzących latach...

Ransomware

Ransomware niezmiennie pozostaje jednym z najbardziej kosztownych zagrożeń dla biznesu, który systematycznie zwiększa nie tylko swoją skalę działania, ale również częstotliwość. Ten rodzaj oprogramowania, ale też technika ataku polega na blokadzie dostępu do danych lub całego systemu komputerowego. Celem jest wymuszenie zapłaty okupu za jego odblokowanie lub odszyfrowanie danych. Stąd też nazwa tego typu programów – ransom, czyli okup, oraz software – oprogramowanie (różne typy tego oprogramowania szyfrującego dokładnie opisuje dokument **Ransomware 2.0.**).

Na początku 2016 roku ransomware uderzał co 2 minuty, rok później co 40 sekund. W 2019 roku mówiono o 14 sekundach, a do 2021 roku czas ten skróci się do 11 sekund! Podczas czytania przez Ciebie tego akapitu ktoś właśnie padł jego ofiarą!

W 2020 roku najczęściej atakował ransomware REvil (inaczej Sodinokibi - 15% ataków), Maze (7,7%) i Phobos (7,7,%). Tuż za "podium" uplasowali się autorzy Netwalker (7,1%), Dharma (6,4%) oraz Ryuk (5,1%).

Ile kosztuje ransomware?

Według danych **Cybersecurity Ventures** wartość globalnych szkód spowodowanych przez ransomware jeszcze w 2019 szacowano na 11,5 miliarda dolarów (dla porównania, w 2015 było to 325 milionów!). To samo źródło podaje, że w 2021 roku straty te mogą wynieść... 20 miliardów dolarów, czego nie można wykluczyć zważając na rosnącą skalę ataków.

Do tych kosztów zaliczamy: wartość zniszczonych lub skradzionych danych, koszty przestoju, utraconej produktywności, postępowania karne, szkolenia pracowników i utratę reputacji.

Z badań zebranych przez **Coveware** dowiadujemy się, że przeciętna wartość okupu w Q2 2020 wyniosła 178 tys.dolarów, co stanowi wzrost o 60% w stosunku do pierwszego kwartału.

Rekordowa wartość okupu zażądana w 2020 roku należy do autorów Ragnar Locker ransomware, który w listopadzie uderzył w znanego producenta alkoholi - włoską firmę Campari. Żądanie sięgnęło kwoty...15 milionów dolarów!!! Skąd tak horrendalna suma? Chociażby w wyniku szczególnie pomysłowej techniki wymuszenia okupu. Operatorzy ransomware postanowili wywrzeć nacisk na Campari uruchamiając... kampanię reklamową na Facebooku skierowaną do klientów ofiary. Reklama w bardzo szczegółowy sposób informowała ich o ataku i groziła upublicznieniem danych w sytuacji odmówienia zapłaty przez Campari.

Źródło: **Centrum Bezpieczeństwa Xopero**

Trendy Ransomware - czego możemy się spodziewać

Stare, dobre luki

Z danych Check Point Research wynika, że na przestrzeni Q3 2020 obserwowano wzrost ilości ataków ransomware o 50% w stosunku do pierwszej połowy roku. Szczególnie niepokojący okazał się jednak fakt, że w przypadku 80% obserwowanych ataków w pierwszej połowie 2020 r. przestępcy wykorzystywali luki i błędy zgłaszane i rejestrowane od 2017 r. Co piąty atak jednak dotyczył luk starszych niż 7 lat. To obrazuje skalę korzystania przez firmy z nieaktualnego, podatnego na ataki oprogramowania.

Nie należy spodziewać się rewolucji w samych formach ataków. Powiedzenie “stare, a dobre” świetnie sprawdza się w przypadku ransomware. Ataki typu brute force, credential stuffing, wykorzystywanie podatności i nie aktualizowanego oprogramowania, czy ataki na PowerShell lub niezabezpieczone RDP - wciąż będą bardzo aktywne.

Ransomware + Leakware = podwójne wymuszenie

Double extortion czyli podwójne wymuszenie to stosunkowo nowa, przestępcza technika, która w zawrotnym tempie zyskuje popularność. Polega na kombinacji ataków typu ransomware z leakware. Przestępcy przed zaszyfrowaniem danych ofiary

CENTRUM BEZPIECZEŃSTWA XOPERO

Cyberataki, malware, luki i podatności - gorące newsy ze świata IT w każdy poniedziałek na Twojej skrzynce mailowej. **Zapisz się!**

Oto o czym informowaliśmy w 2020 r.:

REvil ransomware

Hackerzy od REvil informują, że będą wrzucać do sieci dane ofiar

Gang REvil kupuje malware KPOT na hakerskiej aukcji za 6,5 tys. dolarów

eBay dla cyberprzestępców - grupa od REvil wystawia na aukcji skradzione dane

REvil atakuje kancelarię prawną Madonny, Drake’a, Lady Gagi i innych celebrytów

REvil ransomware wykorzystuje lukę w zabezpieczeniach systemu Windows

Maze ransomware

Operatorzy Maze ransomware formują kartel

Przegląd korona-przekrętów tygodnia

Ryuk

Deszyfrator Ryuk uszkadza większe pliki - zapłacisz, ale nie zyskasz

Prosegur, firma od transportu gotówki, pada ofiarą Ryuk

Malware powiązany z Ryuk wykrada tajne dane armii, informacje finansowe...

wykradają poufne informacje, a następnie grożą ich upublicznieniem. Taka podwójna karta przetargowa zwiększa prawdopodobieństwo spełnienia żądań przez ofiarę. Trend ten, zainicjowany przez grupę odpowiedzialną za Maze ransomware, jest obecnie praktykowany przez największych operatorów oprogramowania szyfrującego i sprawia, że każdy atak może skutkować wyciekiem danych. Co więcej, zapłata okupu nie daje już gwarancji bezpieczeństwa - firmy nie mogą być pewne, że cyberprzestępcy faktycznie skasują skradzione informacje, zamiast wykorzystać je ponownie - do dalszego szantażu lub w kolejnych atakach.

W pierwszym kwartale 2020 roku istniały dwie grupy ze stronami do publikowania wykradzionych danych. W Q4 ich liczba wzrosła do 17.

Trend jest niepokojący także z innego powodu - operatorzy ransomware pokazali, że potrafią ze sobą współpracować. Technika double extortion sprawiła, że z konkurentów stali się partnerami biznesowymi. Można więc spodziewać się, że wymiana doświadczeń, praktyk i narzędzi może skutkować jeszcze bardziej niebezpiecznymi i kosztownymi atakami.

Operatorzy Maze formują kartel ransomware

W ciągu ostatnich kilku miesięcy operatorzy ransomware Maze przyjęli nową taktykę. Teraz upubliczniają dane ofiar, które nie opłaciły okupu. W tym celu stworzyli nawet specjalną stronę “Maze news”. Tę taktykę szybko przyjęły inne grupy – obecnie wiadomo o co najmniej siedemnastu aktywnych operatorach ransomware, którzy grożą wyciekiem danych. Platforma ma służyć nie tylko publikowaniu informacji, ale również wymianie doświadczeń. Autorzy Maze zaznaczyli, że zamierzają traktować inne grupy jak partnerów, a nie konkurentów. Możemy spodziewać się, że wskutek połączenia sił, wymianie rad i taktyk oraz scentralizowanej platformie do wycieku danych, przestępcy będą mieli więcej czasu na tworzenie coraz bardziej wyszukanych i skutecznych ataków.

Źródło: **Centrum Bezpieczeństwa Xopero**

Tradycyjne ataki ransomware, jakkolwiek zjadliwe by nie były, dają ofiarom szansę na odzyskanie danych z backupu bez konieczności zapłaty okupu. W przypadku leakware natomiast, ofiary, które posiadały rozwiązanie do tworzenia kopii zapasowych będą mogły odzyskać dane, ale niestety, nie mogą mieć pewności co do ich dalszego losu w rękach cyberprzestępców. Mamy tu do czynienia niemalże z sytuacją tragiczną, bowiem takiej gwarancji nie daje nawet sama zapłata okupu.

Ransomware w czasach Covid-19

Chyba nikt nie zna się na trendach, tak jak cyberprzestępcy, którzy od wielu lat wykorzystują motywy polityczne, ekonomiczne, czy kulturowe w swoich kampaniach. Nic dziwnego, że okazji doszukali się w wybuchu pandemii. Na przykładzie ataków z Covid-19 w tle mogliśmy również utwierdzić się w przekonaniu, że nie można ufać przestępcom na słowo. W początkowym etapie pandemii, najwięksi operatorzy ransomware obwieścili, że nie będą atakować szpitali i instytucji medycznych. Na ataki jednak nie trzeba było długo czekać - **grupa Maze zaatakowała brytyjskie laboratorium**, które pracowało nad stworzeniem szczepionki, podwoiła się ilość ataków na Światową Organizację Zdrowia, Ryuk nie odpuścił szpitalom, a ich śladem podążyli inni. I tak wszystko wróciło do normy - branża medyczna nadal pozostaje ulubionym celem ataków.

W szczytowym czasie pandemii, co tydzień informowaliśmy o nowych, coraz to bardziej kreatywnych pomysłach przestępców na wykorzystanie paniki związanej z COVID-19. W tym czasie korzystali z niej go nie tylko twórcy ransomware, ale i autorzy kampanii spamowych, phishingowych, malware czy szkodliwego oprogramowania na urządzenia mobilne... Stał za takimi zagrożeniami jak Emotet czy Trickbot.

CENTRUM BEZPIECZEŃSTWA
XOPERO

Cyberataki, malware, luki i podatności - gorące newsy ze świata IT w każdy poniedziałek na Twojej skrzynce mailowej. **Zapisz się!**

COVID-19

Hackerzy zarabiają na lęku przed koronawirusem
Przegląd korona-przekrętów tygodnia
Korona-newsów ciąg dalszy
Motyw z koronawirusem, czyli nowa i skuteczna kampania Trickbot
Śledzisz mapę z COVID-19? Uważaj – mogłeś paść ofiarą przestępców!
Przestępcy grożą, że zarażą Twoją rodzinę koronawirusem...

Crimeware-as-a-service

Software-as-a-service (oprogramowanie jako usługa) to niepodważalnie jeden z najbardziej popularnych modeli biznesowych ostatnich lat. Nie umknęło to uwadze cyberprzestępców, którzy właśnie w tym modelu wystawiają swoje "produkty" na sprzedaż na nielegalnych forach. Stąd nazwa Crimeware-as-a-service - i jej odmiany: Malware-as-a-Service, Ransomware-as-a-Service, Phishing-as-a-Service, itd - wszystko jest na sprzedaż. Usługi przestępcze w tym modelu może nabyć każdy - nawet osoba pozbawiona umiejętności technicznych (i to czasami za mniej niż 50 dolarów!).

Skuteczność modelu Ransomware-as-Service pokazały Cerber, Crysis, Cryptowall, Dharma czy wreszcie GrandCrab. Generuje on ogromne zyski dla obu stron - twórców i kupujących. Autorzy tego ostatniego zarobili 150 milionów dolarów, a pojedyncza opłata wahała się w granicach 600-7000 $. Twórcy Cryptowall natomiast wzbogacili się o 320 milionów w ciągu roku (!).

Nieco inny model przyjęli twórcy ransomware Dharma. Postanowili oni dostarczać złośliwe ładunki początkującym oszustom, którzy dopiero rozpoczynają swoją "karierę" w cyberprzestępczym światku. Aspirujący hakerzy płacą zasadniczo niski abonament za usługi ransomware, a zarobionymi pieniędzmi dzielą się z twórcami Dharmy. W ten sposób operatorzy tego ransomware stworzyli sobie sieć działających dla nich wykonawców i freelancerów.

Jednym z najbardziej zyskownych przykładów Malware-as-a-Service z kolei, jest Emotet. Początkowo trojan bankowy dostarczany przy pomocy kampani malspam, dziś - potężny botnet rozprzestrzeniający się głównie za pośrednictwem złośliwych dokumentów wysyłanych pocztą elektroniczną, który służy obecnie do dostarczania na zainfekowane urządzenia innego malware. Choć Emotet znany jest z robienia sobie dłuższych przerw w działalności, w 2020 roku wciąż pozostawał najbardziej aktywnym malware.

Mobile malware

W 2020 roku producenci telefonów i oprogramowania mobilnego, na czele z dostawcami OS - Androidem i iOS - nie mieli czasu na odpoczynek. Smartfony często zastępują komputery, a pracownicy wykonują na nich swoje obowiązki, logują się do firmowych kont, podają za ich pomocą służbowe dane... - nic dziwnego, że trend rozwoju natywnych aplikacji i mobilnego malware ugruntowuje swoją pozycję.

Dotychczas atakujący urządzenia mobilne na wczesnym etapie infekcji zwykle polegali na zewnętrznych sklepach z aplikacjami i błędach użytkowników. Rosnąca świadomość zagrożeń mobilnych (choć wciąż zbyt ograniczona) skłoniła przestępców do wysiłku i poszukiwania dodatkowych wektorów infekcji. W ostatnich miesiącach minionego roku byliśmy świadkami niespotykanego dotąd wzrostu liczby złośliwych aplikacji, którym udało się

ominąć zabezpieczenia Google Play Store.

Jedną z metod wykorzystywanych do ukrycia złośliwego charakteru aplikacji jest użycie natywnych języków programowania. Zamiast używać Javy do tworzenia appek, przestępcy korzystają z natywnego języka Androida, zazwyczaj C lub C++. To z kolei znacznie utrudnia dekompilację kodu i jego identyfikację oraz zmniejsza skuteczność procedur wykrywania złośliwego oprogramowania w Google Play. Takie programy przedostają się do oficjalnego sklepu Google, a następnie mogą być legalnie pobierane przez użytkowników.

Doskonałym przykładem obejścia zabezpieczeń Google Play jest Joker (zwany Bread). Od 2019 roku, kiedy to pojawił się po raz pierwszy, Google usunął już tysiące zmodyfikowanych aplikacji, a te zostały pobrane przez miliony użytkowników. Mimo to, zagrożenie cyklicznie powraca...

Joker, HiddenAds, Haken, Circle, Tekya...to tylko nieliczne z przykładów malware, wykorzystujących natywne implementacje, aby przedostać się do marketplace'u Google. Rzeczywiście, w momencie, kiedy badacze wzięli pod lupę 150 tys. aplikacji, okazało się, że prawie 7% appek w Google Play posiada backdoory...

Inne zagrożenie związane jest z coraz szerszym wykorzystaniem urządzeń mobilnych do zabezpieczenia kont i logowania. Uwierzytelnianie wieloskładnikowe zakłada z reguły potwierdzenie logowania poprzez aplikację, która staje się tokenem programowym lub poprzez kod z wiadomości SMS wysłanej na podany numer telefonu. Ze względu na ten drugi scenariusz, smartfony stają się więc coraz bardziej popularnym celem ataków m.in. SIM-jacking'u czy wykorzystywania exploitów na systemach operacyjnych.

Spear phishing i kampanie spamowe

Phishing, choć jest jednym z wektorów ataków, który dostarcza złośliwe oprogramowanie, ze względu na swoją skalę zasługuje na osobną analizę. Warto rozpocząć ją od krótkiej retrospekcji. Lata temu hakerzy tworzyli bardzo szerokie kampanie, rozsyłane do ogromnej liczby odbiorców. Dopiero później zauważyli, że selektywny dobór ofiar i spear phishing znacznie podnosi wskaźnik sukcesu. Bogactwo danych osobowych, które można swobodnie odnaleźć w sieciach społecznościowych znacznie ułatwia przestępcom zdobycie informacji o ofiarach i ich nawykach, a następnie tworzenie ukierunkowanych

CENTRUM BEZPIECZEŃSTWA
XOPERO

Cyberataki, malware, luki i podatności - gorące newsy ze świata IT w każdy poniedziałek na Twojej skrzynce mailowej. **Zapisz się!**

Joker

Złośliwy Joker wykryty w 24 aplikacjach na Androida
Spyware Joker po raz kolejny wykryty w Google Play

Inne zagrożenia

Setki milionów użytkowników Androida narażonych na stary błąd – podatne 8% wszystkich appek
Trojan Ghimob szpieguje 153 aplikacje bankowe na Androida na całym świecie
HiddenAds malware znaleziony w 21 aplikacjach z 8 milionami pobrań z Google Play
Malware GravityRAT po raz kolejny pokazuje zęby – teraz atakuje również urządzenia Android oraz macOS
Alien – ten obcy kradnie dane z 226 popularnych aplikacji – w tym w Polsce
VPN na Androida z 100 mln pobrań umożliwiał ataki MITM. Teraz znika z Google Play

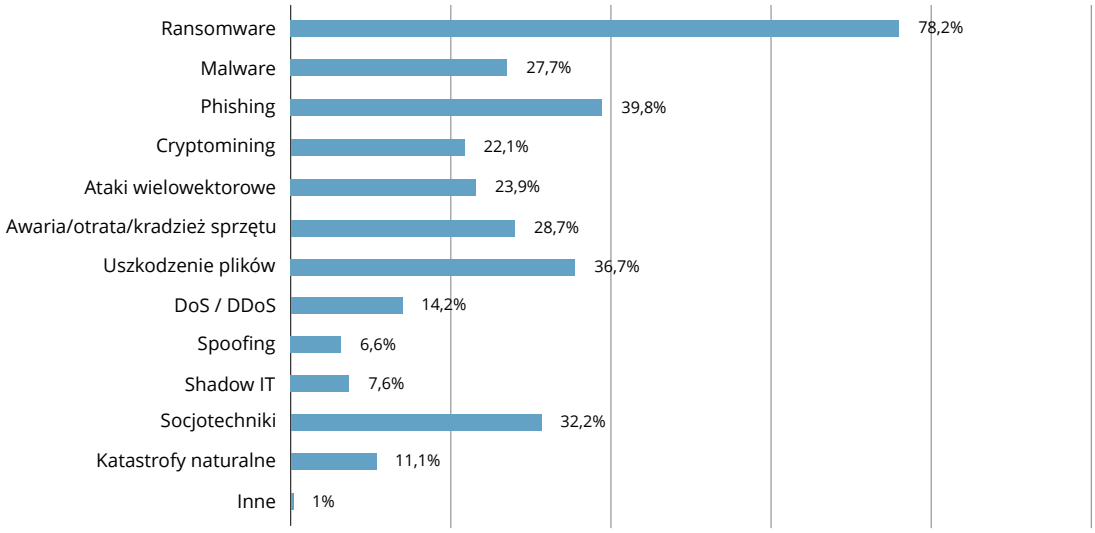
kampanii.

Spoglądając jednak na działania przestępców z 2020 roku nie sposób odnieść wrażenia, że wybuch pandemii przywrócił im możliwości targetowania całych rzeszy ludzi, trafiania do nich ze spersonalizowanym komunikatem nie obniżając jednocześnie skuteczności. Bo COVID-19 bał się niemal każdy, a poziom dezinformacji sięgał zenitu. Generalnie można było odnieść wrażenie, że cyberprzestępczość przybiera nową formę - korona-przestępczości w skali przemysłowej.

Lockdown'owi zaczął więc towarzyszyć spam. Najlepsze tego typu kampanie wymuszają natychmiastową reakcję odbiorcy na komunikat. Wynika to z prostej, psychologicznej sztuczki - jeżeli odbiorca pochyliłby się chwilę dłużej nad treścią wiadomości, prawdopodobnie zauważyłby, że jest fałszywa. Strach i panika powodują jednak, że człowiek szybciej działa, niż myśli. 2020 rok i wybuch pandemii sprawił, że spamerzy nie musieli nawet zbytnio się starać, aby osiągnąć swój cel.

Eksperci ostrzegali również przed wzrostem liczby przynęt socjotechnicznych w złośliwych wiadomościach e-mail. Przestępcy obiecywali ofiarom ulgi finansowe podczas pandemii. Tematami tych wiadomości były rządowe pakiety pomocy finansowej, a nawet czek na 1000$ od Donalda Trumpa, dla osób, które straciły pracę. W Australii przestępcy powoływali się na znane czasopisma, w Wielkiej Brytanii podszywali pod banki oferujące pomoc finansową. Celem były też firmy IT, do których "pisało" samo WHO czy Międzynarodowy Fundusz Monetarny.

Jakich cyberzagrożeń obawiasz się najbardziej?
Źródło: Xopero Software



Jeżeli spojrzymy na rok 2020 z perspektywy szeroko rozumianego bezpieczeństwa możemy dojść do wniosku, że niemożliwym jest, aby przewidzieć i być przygotowanym na wszelkie możliwe zagrożenia. Jestem przekonany, że nie ma na świecie przedsiębiorstwa, czy choćby jednej osoby, która była w pełni przygotowana na globalną pandemię i światowy lockdown.

Sytuacja na świecie w 2020 roku, szczególnie na początku, była bardzo dynamiczna, a firmy musiały wykazać się dużą elastycznością, by dostosować się do tak szybko zmieniających się realiów. Jednym z największych wyzwań dla pracodawców oraz pracowników była zmiana miejsca pracy z siedziby firmy na domowe zacisze. Jednocześnie jest to również jedno z największych wyzwań dla sektora bezpieczeństwa IT – możliwość zapewnienia bezpiecznego dostępu do niezbędnych danych, aplikacji i usług dla pracowników zdalnych w bardzo krótkim czasie. W niektórych przypadkach administratorzy mieli zaledwie kilka dni, by przygotować firmę do pracy zdalnej, a jak dobrze wiemy – pośpiech nie jest sprzymierzeńcem w walce o bezpieczeństwo. Jednymi z najpopularniejszych narzędzi wykorzystywanych do pracy zdalnej są VPN oraz RDP (usługa pulpitu zdalnego) i to właśnie one były jednymi z najczęstszych celów ataków już na początku 2020 r. W większości przypadków administratorzy spisali się na medal, lecz nie obyło się bez głośnych ataków ransomware i tak już na początku lutego, ogromne przedsiębiorstwo logistyczne, jakim jest Toll IT padło ofiarą ataku. W rezultacie ponad 1000 serwerów w 50 krajach na całym świecie zostało zaszyfrowanych. Atak odczuli również klienci firmy, którzy w niektórych regionach świata nie byli w stanie wysyłać, czy śledzić przesyłek. Mówi się, że nic dwa razy się nie zdarza, niestety, mimo że Toll IT uporało się z lutowym atakiem MailTo, inny ransomware (Nefilim) uderzył w nich ponownie w maju. Przestępcy doskonale wykorzystują sytuację, jaka zapanowała na świecie i z pewnością liczba ataków, ukierunkowanych w stronę usług szczególnie popularnych w czasie pracy zdalnej, będzie wzrastać. Jednym z takich przykładów są usługi w chmurze, względnie bezpieczne, ale wielu producentów z segmentu security, przygotowało nowe rozwiązania, by podnieść bezpieczeństwo korzystania z chmury.

Globalny lockdown zmienił wiele naszych przyzwyczajeń, zostajemy w domach ze względów bezpieczeństwa, nosimy maseczki, dezynfekujemy ręce. Ograniczyliśmy nasze spotkania w świecie rzeczywistym, przenosząc je do świata wirtualnego, a to zwiększyło ilość informacji, jakie codziennie wymieniamy drogą elektroniczną i stało się doskonałą pożywką dla przestępców. Niezmiennie od lat phishing email wiedzie prym wśród wektorów ataku ransomware, tak i w tym roku się to nie zmieniło. Zdecydowanie przyczynił się do tego fakt, że wysyłamy i odbieramy dużo więcej wiadomości email, a same kampanie phishingowe dużo lepiej docierały do określonych grup odbiorców. Najczęściej można było usłyszeć o kampaniach, w których przestępcy podszywali się pod wiadomości od firm kurierskich, w których znajdowały się fałszywe odnośniki do śledzenia paczek, czy wysyłali informacje

z koniecznością dopłaty do przesyłki. Nasiliły się również ataki phishing SMS, a te z kolei zdecydowanie przyczyniły się do wzrostu popularności malware dla urządzeń mobilnych i nie powinniśmy zapominać o ich bezpieczeństwie.

W sposobie działania samego ransomware za wiele się nie zmieniło. Niestety wciąż nie potrafimy skutecznie radzić sobie z atakami, które obserwujemy od lat, więc przestępcy nie mają potrzeby obecnie znaczących zmian w tym zakresie. Ataki zdecydowanie jednak przybierają i będą przybierały na sile, dzięki popularności ransomware – dzisiaj niemal każdy z nas może zakupić usługę ransomware w modelu SaaS, wystarczy trochę czasu i pomoc Google, to nic trudnego (to nie jest zachęta). Przestępcy stali się również bardziej wyrafinowani i znaleźli nowe sposoby, by zwiększać prawdopodobieństwo zapłaty okupu przez ofiarę. Jednym z takich sposobów jest wykradanie danych przed ich zaszyfrowaniem, by następnie grozić ofierze ich upublicznieniem. Okazuje się, że sama kopia danych to za mało, ponieważ samo odzyskanie danych nie pomoże zachować reputacji firmy i uniknąć kar (choćby z tytułu GDPR), gdy te mogą zostać w każdej chwili upublicznione. Niestety, nikt nie daje gwarancji, że po opłaceniu okupu dane zostaną skasowane i nigdy nie będą opublikowane. Innym przykładem wywierania nacisku na ofiarę jest równoległe prowadzenie ataku DdoS na strony ofiary, które stają się niedostępne. Firma traci nie tylko dane, ale także swoją wizytówkę w sieci.

W roku 2021 nie spodziewałbym się znaczącego przewrotu jeśli chodzi o sposoby ataków i metody działania przestępców, ale z pewnością ich liczba będzie nadal rosła, a skutki będą stawały się coraz bardziej odczuwalne. Tak samo, jak przestępcy, tak też producenci z branży security będą się zbroić i z pewnością pojawi się kilka interesujących rozwiązań na rynku, które mogą zmienić nasze podejście do postrzegania bezpieczeństwa.

Grzegorz Bąk
Product Development Manager, Xopero Software

W 2020 roku gwałtownie wzrosły kwoty żądanego przez przestępców okupu. Średnia jego wartość wynosi obecnie 233 817 dolarów. To prawie trzy razy więcej, niż rok temu (średnio 84 116 dolarów). Hakerzy zdają sobie sprawę jak kosztowne są dla firm przestoje oraz utrata czy wycieki danych, dlatego stale przesuwają granicę i testują możliwości finansowe ofiar. Ma to miejsce głównie w atakach wymierzonych w duże firmy czy instytucje publiczne. Żądania w stosunku do małych firm czy użytkowników prywatnych pozostają na podobnym poziomie.

W mijającym roku nie powiodło się kilka zaawansowanych, sprofilowanych ataków ransomware na okręgi szkolne w USA. Ich działy IT utrzymywały zapasową kopię wszystkich krytycznych danych, zagrożenie szybko więc zneutralizowano. Rosnąca świadomość firm i instytucji publicznych sprawia, że przestępcy szukają nowych sposobów żądania okupu. W nadchodzącym roku nie tylko będą szyfrowali dane, ale też wykradali wrażliwe informacje i grozili ich upublicznieniem, jeśli żądania nie zostaną spełnione. Zwiększy to presję aby zapłacić okup, nawet jeśli ofiary będą miały kopie zapasowe danych, przechowywane bezpiecznie poza siecią.

Do wykradania informacji z systemów przestępcom coraz częściej będą służyły powszechnie znane, wiarygodne narzędzia, takie jak Total Commander (menedżer plików), 7zip, WinRAR czy Windows cURL, z których korzystają na co dzień także firmy. Dzięki temu przestępcy będą mogli poruszać się po sieci i wyłączać kolejne elementy systemu (takie jak m.in. możliwość tworzenia zapasowych kopii) bez wykrycia, aż do momentu uruchomienia złośliwego oprogramowania. Jednocześnie utrudni to analizę incydentów, gdyż takie działania nie są automatycznie oznaczane przez rozwiązania ochronne jako zagrożenie. W procesie reagowania na incydenty wzrośnie więc rola specjalistów ds. cyberbezpieczeństwa. Ich wiedza i doświadczenie będą ułatwiały wyłapywanie anomalii sugerujących podejrzaną aktywność.

Cyberprzestępcy wykorzystujący ransomware automatyzują ataki. Coraz częściej dzielą się też między sobą narzędziami. Ich łatwa dostępność na czarnym rynku sprawia, że także w nadchodzącym roku stale rosła będzie aktywność początkujących hakerów, którzy wykorzystują głównie oprogramowanie umożliwiające atakowanie dużej liczby mniejszych celów. Stale udoskonalane będą techniki i narzędzia, a gdy jedno zagrożenie zniknie, w jego miejsce szybko pojawiać się będzie kolejne. W 2020 roku hakerów nie powtrzymał nawet kryzys w ochronie zdrowia oraz systemie szkolnictwa związany z epidemią koronawirusa – wielu z nich obierało na cel instytucje z sektora zdrowia i edukacji. Nie można więc liczyć na żadną „taryfę ulgową", ale nieustannie rozwijać metody zapobiegania i reagowania na pojawiające się zagrożenia.

Łukasz Formas
Kierownik zespołu inżynierów, Sophos

Od wielu już lat obserwując cyberzagrożenia na rodzimym poletku i na świecie, można być pewnym jednego - to co znamy i na co jesteśmy gotowi dzisiaj jutro będzie nieaktualne. Codziennością stał się fakt, że kiedy już nauczymy się wykrywać kolejny downloader przechodzący przez filtry mail gateway'a i omijający zabezpieczenia stacji lokalnej, kiedy właśnie wzbogacilismy alertowanie w SOC o logi sysmona i łapiemy oddech nagle okazuje się, że „nieistotne środowisko testowe" nie dość, że połączone bezpośrednio ze środowiskiem produkcyjnym to „zupełnie przypadkowo" znalazło się w internecie. Brzmi znajomo? I dobrze. Brak incydentów zazwyczaj nie świadczy o doskonałej kondycji środowiska IT ale o tym, że ich po prostu nie wykrywamy. Gorsza wiadomość jest taka, że doskonale robią to za nas cyberprzestępcy...

Rok 2020 nie był tu wyjątkiem, giganci padali ofiarą ransomware (Garmin, Randstad, Capcom, Software AG i inni), na Tianfu Cup standardowo udało się skompromitować najnowsze wersje Chrome, Firefox, VMWare ESXi i Windows 10. Padły również zabezpieczenia najnowszego iPhone, Galaxy S20 i ostatnie modele IoT popularnych producentów. Nie inaczej było z odkrytymi na przestrzeni roku najgroźniejszymi podatnościami, wspomnieć choćby RCE w MS Teams, VMWare, Citrix SD-WAN, Discord czy Slack - a to tylko kilka z co najmniej kilkudziesięciu.

Z kolei na nasze prywatne pieniądze i dane dostępowe do naszych kont (nie tylko mailowych czy społecznościowych) stale czyhają zmyślnie konstruowane i regularnie odświeżane kampanie phishingowe. Na stałe już w Polsce zadomowiły się złośliwe SMSy wysyłane na przeróżne sposoby, vishing (włączając w ten proceder CLI spoofing), setki facebook scamów miesięcznie żerujących na naszej odwiecznej ciekawości, obiecujące góry złota serwisy kryptowalut i „inwestycje w Amazona" okraszone fake newsami ze znanymi polskimi celebrytami bądź przypadkowymi osobami, które porzuciły pracę bo zarabiają kilkanaście tysięcy zł tygodniowo nic nie robiąc. Niby śmieszne a proceder trwa w najlepsze i ludzie wpłacają tam ciężko zarobione pieniądze.

Nie może też zabraknąć nowych metod w przestępczym arsenale. Tutaj zdecydowanie wybijają się „oszustwa na OLX" polegające na kontakcie przestępców via Whatsapp pod pozorem zakupu wystawianych przedmiotów i oferujących zakup z dostawą. Scenariusz opiera się o podesłanie fałszywego linku pod pozorem uzyskania zapłaty/zwrotu za dostawę i kradzież danych karty płatniczej. Co więcej, przestępcy byli tak kreatywni, że przygotowali nawet własne grafiki (!) brandowane OLXem pokazujące ofiarom jak korzystać z tej nowej funkcjonalności... I nie dać się oszukać! Wspominałem o monitoringu sieci za pomocą Solarwinds Orion?

Robert Grabowski
Kierownik Wydziału CERT, Orange Polska

W roku 2020 niemal za wszystko można winić pandemię: postępującą inflację, kiepski stan ekonomii, prognozy PKB. Stan odporności firm na ataki cybernetyczne również nie stanowi tutaj wyjątku.

Bądźmy szczerzy: praca zdalna nigdy nie była polską specjalnością. Przedsiębiorcy od lat eksperymentowali z różnymi formami „home office", jednak nie byli przygotowani na oddelegowanie np. połowy pracowników do swoich domów.

Według danych GUS i Eurostatu, ilość osób pracujących zdalnie niemal się potroiła w ciągu jednego kwartału. W czwartym kwartale 2019 r. tylko 4,3 proc. Polaków wykonywało swoją pracę zdalnie. Natomiast w pierwszym kwartale 2020 r., już 11 proc. Ta raptowna migracja połączona z pandemią przyniosła wiele negatywnych skutków dla przedsiębiorstw.

Po pierwsze, COVID spowodował wylew nowych ataków socjotechnicznych rozprowadzanych drogą mailową lub wiadomościami SMS. Najwięcej ucierpiały na tym Włochy, gdzie hakerzy wykorzystywali element chaosu informacyjnego do tworzenia stron internetowych zainfekowanych złośliwym oprogramowaniem. Te natomiast szpiegowały użytkowników i instalowały malware. U nas popularną metodą na wyłudzanie danych stały się ataki smshingowe, informujące internautów o dodatkowych opłatach związanych z koronawirusem – np. za rzekomą dezynfekcję paczki.

Drugą zmianą spowodowaną sytuacją pandemiczną było uzewnętrznienie usług intranetowych przez firmy. Tutaj pośpiech był najgorszym doradcą, ponieważ część firm domyślnie skorzystała z technologii split-tunnel VPN, zamiast pełnego VPN, który z natury obciąża infrastrukturę firmy. Split-tunnel VPN to rozwiązanie, które pozwala zdalnemu urządzeniu na łączenie się z usługami wewnętrznymi jednocześnie pozwalając na bezpośrednie łączenie się z internetem. Z punktu widzenia ochrony danych ten typ VPN jest dość problematyczny, ponieważ ruch internetowy pozostaje poza zasięgiem systemów monitorujących, a tą drogą często dochodzi do wycieków danych.

Samo przygotowanie hardware'u również sprawiło przedsiębiorcom wiele kłopotów. Niejednokrotnie w ruch poszły przestarzałe urządzenia, jak najszybciej przygotowane do pracy. Choć według litery prawa pracodawca powinien przygotować miejsce pracy, część osób pracujących zdalnie wykorzystywała swoje urządzenia, np. routery i switche. Te znów stały się celem zwiększonych ataków hakerskich, ponieważ drobne zmiany w konfiguracji urządzeń infrastruktury zdalnej rzadko kiedy bywają zauważone (natomiast sam temat, czy pracodawca powinien wyposażyć pracownika w routery nie jest jasny).

Jednocześnie w ostatnim roku najbardziej ewoluował ransomware. Choć ten typ złośliwego

oprogramowania towarzyszy nam od lat, z końcem 2019 r. grupy cyberprzestępców wpadły na nowy pomysł jak wymuszać opłacenie okupu: metodę „name and shame”. Ta metoda stała się niemal standardem w 2020 r. Po zainfekowaniu urządzeń, kopia danych jest automatycznie wysyłana do hakerów, a później szyfrowana. Jeżeli ofiara nie zapłaci okupu, hakerzy informują media o ataku i wycieku danych, niszcząc reputację firmy i narażając na kary związane z RODO.

W związku z powyższym, najlepszą poradą na 2021 r. jest zwrócenie uwagi na ataki socjotechniczne i niezależne audyty bezpieczeństwa. Im więcej osób pracuje zdalnie, tym mniejszą mamy kontrolę nad przepływem danych.

Paweł Wałuszko
Cybersecurity Expert, TestArmy

Rok 2020 będzie zapamiętany jako przełomowy. Firmy, które nie wyobrażały sobie pracy innej, niż biurowa w siedzibie firmy nagle zostały postawione przed wymogiem pracy zdalnej. Jednak największe wyzwanie zostało postawione przed pracownikami działów IT. Nagle trzeba było zorganizować pracownikom sprzęt i co gorsza, dostęp do zasobów firmy. Firmy, które w ostatnich latach przespały możliwości wdrożenia nowych mechanizmów pracy zdalnej i rozproszonej nagle musiały nie tylko przewartościować swoje podejście do pracy, ale też zainwestować spore sumy w takie zmiany. A te niosły za sobą wzrost zagrożeń dla bezpieczeństwa firmowych danych. Po pierwsze problem połączeń - nie wszyscy od początku korzystali z VPN i sensownych metod uwierzytelniania zdalnych pracowników. Po drugie, znacząco wzrosły ataki związane z ransomware. O ile pracując z biura każdy pracownik był potencjalnie za firmowymi zaporami, pod kontrolą firmowych polityk zabezpieczeń, o tyle przy pacy zdalnej bywa z tym gorzej. Wiele firm bardzo mocno broniło się przed trendem Bring Your Own Device, a tu nagle sytuacja się odwróciła i zamiast pojedynczych urządzeń w sieci firmowej, nagle mieliśmy większość urządzeń poza nią. Tak więc głównie trzeba było polegać na świadomości użytkowników. Niestety, również na niej polegali atakujący. A dokładniej na jej braku.

Jak więc w takich realiach zapewnić bezpieczeństwo danym? Teoretycznie każdy ma backup, ale jak go teraz wykonywać, gdy pracownicy są poza firmową siecią? Dlatego trzeba było przejść na zdalną pracę na scentralizowanych danych. I tutaj pojawia się kwestia skutecznego ich zabezpieczenia. Każdy użytkownik zdalny podłączony do firmowej sieci staje się potencjalnym źródłem infekcji ransomware. W tej sytuacji administratorzy musieli szukać dodatkowych metod zabezpieczenia firmowych serwerów. Takim idealnym mechanizmem są migawki. Nie jest to backup, ale mechanizm, który możemy uznać za „ostatnią deskę ratunku". Jeśli dane zostaną zaszyfrowane, może się okazać, że wśród niedostępnych już plików będą też pliki z kopiami bezpieczeństwa. Mechanizm migawek pozwala chronić dane na poziomie bloków przed modyfikacjami. Gdy tworzona jest migawka danych, określona wersja tych danych z konkretnego punktu w czasie zostaje „zamrożona". Pracując na plikach, wprowadzając dowolne zmiany, są one zapisywane w innych blokach. W ten sposób nawet, jeśli wszystkie dane zostaną zaszyfrowane, będziemy mieli możliwość przywrócenia ich z migawki. Sama migawka powinna być niedostępna z poziomu systemu plików oraz chroniona przed dostępem z sieci. Tylko wtedy możemy uznać ją za bezpieczną i chroniącą dane naszej firmy przed ransomware.

Łukasz Milic
Business Development Representative, QNAP Systems

Rynek cyberbezpieczeństwa w Polsce jest ciągle relatywnie niewielki i na stosunkowo wczesnym etapie rozwoju. Po latach dynamicznych wzrostów rok 2020 przyniósł niewielkie spadki, wywołane głównie zamrożeniem budżetów na inwestycje związane z wybuchem pandemii COVID-19. Niemniej jednak w najbliższych latach prognozowane jest odbicie i powrót na ścieżkę wzrostów. Sytuacja w Polsce wpisuje się w trendy globalne, gdyż na największych rynkach takich jak USA czy Chiny również nastąpiło spowolnienie, ale jest ono przejściowe. Niedawne doniesienia o ogromnym włamaniu do kluczowych systemów bezpieczeństwa administracji w Stanach Zjednoczonych tylko zwiększy presję na zwiększenie nakładów na rozwój odpowiednich narzędzi mających zapobiec podobnym incydentom w przyszłości.

Polskie firmy z branży cyberbezpieczeństwa są nastawione przede wszystkim na świadczenie usług, niewiele jest natomiast podmiotów posiadających w ofercie interesujące produkty o globalnym potencjale na rozwój. Przedsiębiorstwa zmagają się również z wieloma wyzwaniami. Wg badania przeprowadzonego przez fundusz Venture INC, największym z nich jest ciągle relatywnie niska świadomość rynkowa dotycząca konieczności stosowania rozwiązań z zakresu cyberbezpieczeństwa. Eksperci podkreślają, że firmy w Polsce są pod tym względem kilka lat do tyłu w porównaniu do krajów Europy Zachodniej czy USA. Niemniej jednak sytuacja ta się zmienia, na co wpływ niewątpliwie miała również pandemia COVID-19 i związana z nią eksplozja popularności pracy zdalnej. Taki model pracy ma niewątpliwe zalety, ale rodzi również szereg zagrożeń związanych z potencjalnymi podatnościami na cyberataki. Problemami podnoszonymi często w badaniu są również trudności w znalezieniu odpowiednio wykwalifikowanych pracowników, jak również brak wystarczającego kapitału potrzebnego do dynamicznego rozwoju.

Co ciekawe, z badania wynika, iż w przypadku pozyskania finansowania firmy zdecydowanie preferują inwestorów prywatnych (fundusze VC, aniołów biznesu itp.) ponad pomoc publiczną (dotacje, granty). Przewagą kapitału prywatnego jest jego elastyczność, lepsze dostosowanie do potrzeb przedsiębiorców i brak z góry narzuconych kryteriów. Fundusze publiczne obarczone są całą gamą ograniczeń i wymagają dużej inwestycji czasowej do ich rozliczania. Inwestorzy poza pieniędzmi wnoszą też do spółek wartości niematerialne, know-how w postaci sieci kontaktów, doświadczenia biznesowego i mentoringu. To często jest element trudny do zmierzenia, acz niezmiernie ważny dla firm w kontekście ich dalszego rozwoju i globalnej ekspansji.

Tomasz Kryda
Starszy Analityk, Venture INC

Infrastruktura IT jest sercem każdego biznesu – jednak podatnym na różne zagrożenia. Jak chronić sieć przed atakami zewnętrznymi i błędami użytkowników? Częstym zabezpieczeniem są programy antywirusowe, chroniące stacje robocze. Jednak to brzeg sieci stanowi główną bramę przez którą przechodzi ruch sieciowy. Poniżej najważniejsze filary bezpieczeństwa, które warto uwzględnić w ochronie brzegu sieci przed złośliwym oprogramowaniem.

1. Trójsilnikowy system antywirusowy – Skanowanie AV, powinno być oparte o trzy niezależne mechanizmy, kolejno testujące ściągany plik. Celem takiego łańcucha, jest wykrycie znanych oraz nieznanych jeszcze szkodliwych plików. Jeden z silników, powinien umożliwiać behawioralną analizę kodu.

2. Moduł bazujący na reputacji zasobów Internetu. Moduł taki pozwala na prewencyjne zablokowanie komunikacji z zasobami Internetu, znanymi z propagowania szkodliwej zawartości. Jednym ze skutków jego zastosowania, jest zaoszczędzenie zasobów obliczeniowych urządzenia po przez eliminację konieczności skanowania kontentu – który po prostu nie jest pobierany.

3. Kolejny filar to Intrusion Prevention System (IPS). Pod tą nazwą kryje się skaner pakietów, wykrywający próby włamań, opartych o wykorzystanie znanych podatności aplikacji.

4. Ważnym wyzwaniem, które stoi przed administratorem sieci jest również zablokowanie dostępu do określonych witryn WEB, oraz blokada możliwości skutecznego korzystania z określonych grup aplikacji jak np. P2P, TOR, VoIP itp. Moduły kontrolujące aplikację oraz dostęp do witryn WEB, mogą podnieść produktywność w organizacjach i ograniczyć zagrożenia płynące z używania nie których aplikacji.

5. Na brzegu sieci naszych organizacji, zwykle pracuje bramka VPN dla zdalnych pracowników. Jednak korzystanie z VPN, niesie za sobą pewne ryzyko. Jest ono spowodowane tym, że stacja robocza, z której pracownik łączy się z zasobami firmy, może mieć aktywnie działające szkodliwe oprogramowanie. Rozwiązaniem tego problemu może być udostępnienie firmowych aplikacji zdalnemu pracownikowi, na specjalnej witrynie WEB, która może być wystawiona na urządzeniu brzegowym. Dzięki niej, pracownik zdalny nie musi zestawiać połączenia VPN, lecz tylko z pomocą przeglądarki WWW loguje się na tą witrynę i bezpośrednio w oknie przeglądarki uzyskuje dostęp do wewnętrznych WebAplikacji, zdalnych pulpitów albo terminali SSH.

6. Firmowa sieć powinna również posiadać wzmocniony system DNS, który potrafi zabezpieczyć użytkownika, przed połączeniem się z domenami, znanymi z wyłudzania

danych. Taki system – to strażnik, który zamiast umożliwić otwarcie takiej witryny, wyświetla informację o tym, że za blokował taką próbę i tym samym ochronił użytkownika przez możliwością zostania ofiarą phishingu.

Bogusław Gacek

Inżynier wsparcia technicznego rozwiązań WatchGuard Technologies, Net Complex

Luki w oprogramowaniu, systemach IT i urządzeniach sieciowych mają bezpośredni wpływ na realne bezpieczeństwo organizacji. Nie bez powodu patchowanie jest jedną z najważniejszych strategii cyberochrony, ponieważ nic tak nie ułatwia hakerom działania jak niezaktualizowane środowisko IT. Z tego powodu kluczem do bezpieczeństwa jest zrozumienie przeciwnika i uświadomienie sobie, że średnio po **15 dniach** pojawia się pierwszy exploit na ujawnioną podatność w bazach CVE.

Rozważając ryzyko ataku chcę przytoczyć kilka faktów. Po pierwsze procedery atakowania organizacji zdarzają się nagminnie bez względu na finansowe nakłady przeznaczone na cyberbezpieczeństwo. Wyciekały nawet exploity sprzedawane przez firmę Hacking Team (narzędzie Remote Control System do atakowania wszelakich systemów). Wśród zamawiających byli klienci z Bahrajnu, Sudanu, Włoch, Węgier, Czech, Szwajcarii, Rosji, USA, a nawet Polski. Po drugie nie trzeba „rozbijać banku", aby zaszkodzić obranemu celowi. Według firmy Trend Micro cyberprzestępcze usługi takie jak „pay-per-install" to koszt od 100 do 550 dolarów za 1000 pobrań (cenniki można też znaleźć w sieci Tor). Firma Kaspersky Lab podaje, że na jednym z rosyjskich undergroundowych for internetowych próbowano sprzedać exploita obchodzącego wszystkie zabezpieczenia systemów (aż do wersji Windows 10) za 95 tys. dolarów. Po trzecie za kontrowersyjnym procederem pozyskiwania exploitów stoją całkiem legalne firmy m.in. Zerodium. Za podatność typu RCE na desktopy płacą do 1 miliona dolarów. Za podobny exploit dla systemów mobilnych Android/iOS oferują aż do 2,5 miliona dolarów. Handel exploitami ma się dobrze i jako, że rozwija się rynek usług Cybercrime as a Service, zwiększa się także dostęp do exploitów dla początkujących hakerów.

Podsumowując luki w zabezpieczeniach są niczym drzwi do systemów organizacji i poufnych danych. Nie trzeba się znajdować w bezpośrednim kręgu zainteresowań hakerów, aby ponieść finansowe i wizerunkowe straty. Wiele ataków przeprowadzanych jest automatycznie poprzez skanowanie puli adresów IP lub niezabezpieczonych usług internetowych, a więc bez wybierania konkretnego celu (liczy się ilość podatnych celów, a nie jakość ataku). Podczas testów bezpieczeństwa jakie przeprowadzamy w AVLab.pl obserwujemy z jaką łatwością może dojść do zainfekowania urządzenia, jeżeli system lub aplikacje nie będą zaktualizowane. Wystarczy spreparowana strona z exploitem pod konkretną wersję systemu Windows i przeglądarkę. Szczególnie zagrożone są poprzednie generacje serwerów i systemów, ponieważ tam występuje najwięcej powszechnie znanych luk w zabezpieczeniach (łatwiej też o przygotowanie ataku). Stąd moja rekomendacja dla rozwiązań do zarządzania podatnościami.

Adrian Ścibor
Redaktor naczelny, AVLAb

Internet of Things
– nowy, groźny wektor ataku

Rynek rozwiązań IoT jest niezwykle zróżnicowany. Nie istnieje jeden wspólny standard określający przebieg uwierzytelnienia device-to-device lub bezpieczny sposób nawiązywania połączenia z usługami w chmurze. Wiele urządzeń Internetu Rzeczy stworzono z myślą o realizacji bardzo wąskiego zakresu operacji. Niektóre urządzenia mają za zadanie wyłącznie przekazywać informacje. Inne z kolei przechowują w sposób statyczny dane, do momentu, kiedy zostaną w jakiś sposób uruchomione lub wybudzone. Aby działać poprawnie wymagają tylko kilku podstawowych funkcjonalności. Niestety w niektórych przypadkach IoT zostały okrojone do tego stopnia, że kwestia zabezpieczenia zeszła na bardzo daleki plan. Właśnie z uwagi na ten problem, dotychczasowe podejście do cyberbezpieczeństwa nie sprawdza się w kontekście IoT. Dodajmy do tego jeszcze fakt, że 98% całego ruchu pochodzącego z urządzeń IoT nie jest w żaden sposób szyfrowana. I już widać, że świat składający się z 80 miliardów połączonych ze sobą urządzeń to rzeczywistość szczególnie podatna na wszelkiego typu ataki.

Proporcjonalnie ze wzrostem urządzeń Internetu Rzeczy, wzrasta również liczba malware IoT. Specjaliści szacują, że niedługo staną się one jednym z kluczowych zagrożeń – na równi z ransomware, tradycyjnym malware, czy cryptominerami, itp. Wskazuje na to kilka czynników.

Wspomniany wcześniej szybki wzrost liczby urządzeń IoT, mało bezpieczny proces wdrożenia poprzez internet, brak stosownych aktualizacji, czyni urządzenia IoT szczególnie podatne na różnego typu ataki non-zero-day. Na koniec – brak wglądu w stan zabezpieczeń oraz aktywnych procesów samego urządzenia.

W jaki sposób hackuje się urządzenia IoT

Internet jest pełen słabo chronionych urządzeń lub co gorsza, całkowicie odsłoniętych na ataki. Przestępcy systematycznie skanują sieć w poszukiwaniu takich – nie oszukujmy się – łatwych celów. W przypadku IoT skupiają się na poszukiwaniu dwóch rzeczy – usług telnet oraz SSH. W momencie znalezienia takiej odsłoniętej usługi, szkodliwe oprogramowanie podejmuje próbę zalogowania się za pomocą krążących po sieci i dark web danych uwierzytelniających (atak brute-force). Zdarza się również, że sięgają po zdalne exploity aplikacji, które działają na urządzeniach Internetu Rzeczy. Ta metoda ataku jest o tyle przydatna, że przestępcy nie muszą sięgać po exploity typu zero-day.

Operatorzy botnetów nierzadko konkurują ze sobą o to, kto pierwszy zainfekuje i przejmie urządzenia w oparciu o konkretną podatność. Dlatego jak tylko urządzenie znajdzie się w ich rękach, łatają lukę która umożliwiła wdarcie się do systemu. W ten sposób są w stanie zachować nad nim kontrolę na dłużej.

W przeszłości malware IoT przejmowały urządzenia głównie po to by wdrożyć na nich cryptominery. Dziś już tak nie jest. Stało się tak prawdopodobnie z uwagi na fakt, że urządzeniom IoT brakuje odpowiedniej

mocy obliczeniowej i zasobów. Z punktu widzenia przestępców, dużo bardziej opłacalne jest przejmowanie serwerów.

Będąc częścią botnetu urządzenie służy do przeprowadzania zsynchronizowanych ataków DDoS przeciw konkretnym sieciom, aplikacjom web lub usługą DNS. Ogólna siła takiego ataku jest współczynnikiem liczby urządzeń pomnożonym przez przepustowość każdego z nich.

Zabezpieczanie IoT od początku było problemem, który z biegiem czasu tylko przybrał na sile. Dlaczego malware IoT rozprzestrzeniają się z taką łatwością? Ma na to wpływ fakt, że wiele usług jest dostępnych z poziomu internetu. Dlatego zanim wdrożysz nowe rozwiązanie IoT zweryfikuj czy twoja sieć jest podatna na tego typu ataki a jeśli tak, ogranicz się tylko do usług które są konieczne dla zachowania operacyjności Twoich urządzeń.

Jeśli tylko jest to możliwe, urządzenia IoT – ich usługi - nie powinny być dostępne z poziomu internetu. Ataki supply chain są bardzo trudne do wykrycia - jest to szczególnie problematyczne właśnie przy IoT. Administrator IoT posiada niestety stosunkowo ograniczony wgląd w to jakie oprogramowanie wykonuje operacje na danym urządzeniu.

Organizacje niejako zaakceptowały fakt, że ich urządzenia funkcjonują na zasadzie czarnej skrzynki. Pełna widoczność sieci oraz monitoring urządzeń Internetu Rzeczy są jednak konieczne do tego by chronić organizację przed atakami, których wektorem są właśnie IoT.

Jak monitorować w takim razie urządzenia IoT? Choćby za pomocą rozwiązań OT/IoT. Rozważmy sytuację gdy aktualizacja oprogramowania układowego zawiera złośliwy kod. Jeśli organizacja dysponuje rozwiązaniem do wykrywania i monitorowania zagrożeń w czasie rzeczywistym, wychwyci ono moment, w którym urządzenie zaczyna wykazywać złośliwe (atypowe) operacje. W kolejnym kroku program skoreluje zdarzenie z aktualizacją a na koniec administrator otrzyma stosowny alert.

Rekomendacje

I. Unikaj udostępniania urządzeń IoT w ramach publicznej sieci. Dokładnie oceń stan bezpieczeństwa swoich urządzeń oraz - o ile istnieje taka możliwość - wdróż rozwiązanie monitorujące.

II. Ogranicz usługi do tych, które są ściśle wymagane dla zachowania operacyjności urządzenia – nawet w sytuacji, gdy IoT działa wyłącznie w ramach sieci wewnętrznej.

III. Zweryfikuj u vendora, czy nieudokumentowany mechanizm zdalnego dostępu został wyłączony.

IV. Jeśli to możliwe, wyłącz opcję nawiązywania zdalnego dostępu z urządzeniem.

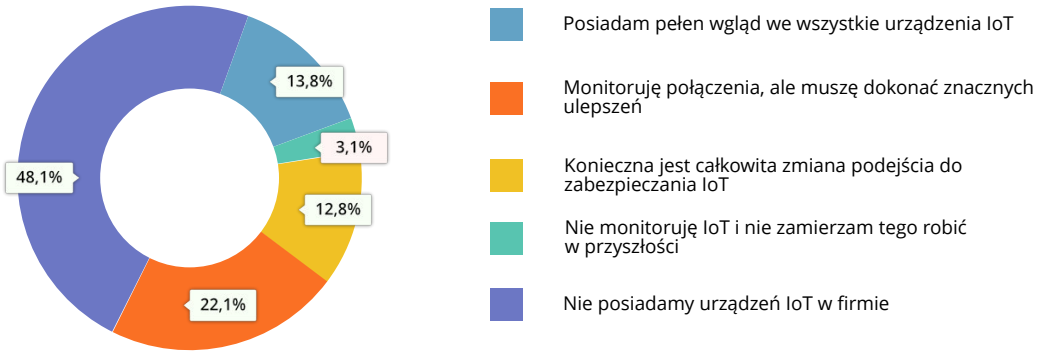
Nie zabezpieczysz czegoś, czego nie widzisz

95 procent osób na stanowiskach decyzyjnych w działach IT jest przekonana, że posiada wgląd we wszystkie urządzenia IoT łączące się z firmową siecią. Tylko 4 procent uważa, że nie ma potrzeby ulepszania obecnie stosowanych metod zabezpieczania. Ponad połowa respondentów przyznaje jednak, że albo musi dokonać znacznych ulepszeń (41 procent), albo że konieczna jest całkowita zmiana podejścia do zabezpieczania IoT (17 procent). Specjaliści zwracają również uwagę na wzrost i większą różnorodność samych urządzeń - connected-cars (27 procent), connected toys (34 procent) i urządzeń medycznych typu wearable (44 procent). Przy tym stwierdzają również, że 57 procent urządzeń IoT jest podatnych na ataki o średniej lub dużej sile.

Skala i tempo wdrożeń urządzeń IoT stanowi problem sam w sobie. Większość respondentów – bo aż 89 procent zgłosiła, że zauważyła znaczny wzrost liczby urządzeń IoT w swoich sieciach w ciągu ostatnich 12 miesięcy.

Jak na podobne pytania odpowiadają polscy specjaliści IT? Z danych zebranych przez Xopero Software dowiadujemy się, że ponad 22 procent ankietowanych

Jak oceniasz wgląd w status urządzeń Interentu Rzeczy, które łączą się z firmową siecią?
Źródło: Xopero Software



przyznaje, że monitoruje połączenia pomiędzy urządzeniami Internetu Rzeczy, ale musi jednak dokonać znacznych ulepszeń. Ponad 12 procent musi całkowicie zmienić swoje podejście do zabezpieczania IoT. Tylko 3 procent ankietowanych nie prowadzi monitoringu urządzeń IoT. Co okazało się największym zaskoczeniem - prawie 48 procent ankietowanych stwierdziło, że nie posiada urządzeń IoT w firmie.

Jak zabezpieczać infrastrukturę IoT

1. Namierz i skataloguj wszystkie urządzenia IoT, jakie występują w ramach sieci.

Nie jesteś w stanie zabezpieczać czegoś, czego nie widać. Profilowanie wszystkich urządzeń IoT zapewni Twojemu zespołowi ds. bezpieczeństwa IT konieczny wgląd w niezarządzane zasoby w ich środowisku IoT: dokładną liczbę podłączonych do sieci urządzeń IoT i ich bazowe systemy operacyjne, profile ryzyka i zachowanie podczas interakcji z innymi podłączonymi urządzeniami. Ten krok ma kluczowe znaczenie dla zabezpieczenia IoT.

2. Systematyczne wgrywanie aktualizacji oraz łatanie podatności.

Większość urządzeń IoT nie projektowano z myślą o przeprowadzaniu regularnych aktualizacji zabezpieczeń. Zespoły IT powinny na bieżąco monitorować stan dostępnych aktualizacji. W celu ograniczenia wystąpienia utraty danych lub kontroli nad urządzeniem warto zaimplementować IoTAware i ochronę przed zagrożeniami internetowymi.

3. Segmentacja urządzeń IoT

Zaimplementuj mikrosegmentację w swojej sieci za pomocą odpowiedniej konfiguracji VLAN i zapory sieciowej nowej generacji aby odizolować urządzenia IoT od innych zasobów IT. Przy odpowiedniej konfiguracji – w momencie wystąpienia ataku - można ograniczyć go do określonego fragmentu sieci.

Sieć powinna być podzielona w oparciu o typ urządzenia, poziomy zagrożeń, wzorce użytkowania oraz inne dostępne cechy profilu urządzenia. Następnie konieczna jest dalsza segmentacja według przyjętych poziomów bezpieczeństwa. Takie postępowanie stworzy silną ochronę obwodową, zmniejszy zakres ataku i ograniczy boczny ruch exploitów.

4. Polityka haseł

Silne hasła stanowią podstawę, bez znaczenia czy mówimy o ochronie konta Microsoft 365, czy zabezpieczaniu IoT. W momencie, gdy nowe urządzenie IoT nawiązuje po raz pierwszy połączenie z siecią, administrator powinien zastąpić słabe

domyślne hasło, nowym – zgodnym z wewnętrzną polityką bezpieczeństwa.

5. Włącz aktywne monitorowanie w czasie rzeczywistym

Tradycyjne rozwiązania EDR (endpoint detection and response solutions), wymagają agentów, są więc nieskuteczne w kontekście zabezpieczenia IoT. W przypadku większości urządzeń Internetu Rzeczy nie jest możliwe instalowanie na nich nowego, dodatkowego oprogramowania. Zamiast tego specjaliści doradzają zaimplementowanie rozwiązania monitorującego, które stale analizuje zachowanie wszystkich punktów końcowych IoT połączonych z siecią w czasie rzeczywistym.

Ustal tzw. trusted behaviors, w ten sposób szybciej wychwycisz zachowania będące anomalią. Integracja z systemem bezpieczeństwa i stały monitoring będą również przydatne w kontekście analizy urządzeń poddanych kwarantannie.

Shadow IoT

Enterprise wykorzystuje rozwiązania mobilne na coraz większą skalę. Granica pomiędzy sprzętem firmowym, a komputerem domowym, czy pracą w firmie, a pracą z domu zaczęła się niebezpiecznie zlewać. Także obecna pandemia odegrała w tym niemałą rolę. W wielu przypadkach administratorzy nie są nawet świadomi wielkości ruchu jaki generują urządzenia IoT. Ta nowa niepokojąca zmiana – nazywana przez specjalistów shadow IoT – stwarza możliwość ataków z wykorzystaniem wektorów, których wcześniej nie brano pod uwagę.

Ruch generowany przez urządzenia Internetu Rzeczy rośnie w zatrważającym tempie. Według **danych zebranych przez Zscaler ThreatLabZ** do maja 2019 r. miesięcznie odnotowywała 56 mln transakcji IoT. Do lutego 2020, ta liczba wzrosła do 33 mln dziennie, co w przeliczeniu dało 1 mld w ciągu całego miesiąca. Mówimy więc o wzroście w granicach 1500 procent. Wraz ze wzrostem ruchu, wzrosła również liczba ataków malware IoT. W maju 2019 Zscalar zablokował 2 tys. zagrożeń wyposażonych w moduły malware. W lutym kolejnego roku liczba ta wyniosła już 14 tys. na miesiąc.

Najpopularniejsze kategorie urządzeń IoT zidentyfikowane przez Zscaler to terminale do gromadzenia danych, odtwarzacze multimedialne, przemysłowe urządzenia kontrolne, urządzenia medyczne, urządzenia sieciowe, terminale płatnicze i drukarki. Analiza ujawniła jeszcze jedną ciekawą informację. Część ruchu pochodziła od nieautoryzowanych urządzeń IoT, takich jak domowi asystenci, dekodery telewizyjne, kamery IP, urządzenia będące częścią inteligentnego domu, Smart TV, Smart Watche, a nawet samochodowe systemy multimedialne.

Wiele nam to mówi o zachowaniu samych pracowników. Będąc zalogowanymi do firmowej sieci, sprawdzają m.in. domowe kamery monitoringu, przeglądają służbową pocztę z poziomu Apple Watch, czy zmieniają ustawienia termostatu. Około 83% transakcji opartych na IoT odbywa się za pośrednictwem zwykłych kanałów plain text, podczas gdy tylko 17% korzysta z SSL.

W odpowiedzi na rosnące zagrożenie, przedsiębiorstwa powinny skupić się na uzyskaniu wglądu w nieautoryzowane urządzenia IoT działające w ich sieci. Tym bardziej, że niektóre urządzenia nie przestrzegają odpowiednich praktyk bezpieczeństwa, co czyni je podatnymi na ataki. W dalszym kroku administratorzy powinni ograniczyć dostęp urządzeń z sieci zewnętrznych, zmienić domyślne poświadczenia, wymagać stosowania silnych haseł i przeprowadzać aktualizacje zabezpieczeń oraz oprogramowania. Poniżej przedstawiono problemy bezpieczeństwa najczęściej obserwowane przez badaczy Zscalera:

1. Komunikacja HTTP serwer/firmware w formie plain text.
2. Uwierzytelnianie HTTP w formie plain text.
3. Korzystanie z nieaktualnych wersji bibliotek.
4. Słabe fabryczne dane uwierzytelniające.

Zabezpieczanie urządzeń 5G

Urządzenia działające w sieci 5G wymagają odmiennych metod zabezpieczania

Według szacunków SMU Office of Research&Tech do końca 2024 roku całkowity mobilnych ruch danych osiągnie zawrotną wielkość 131 eksabajtów miesięcznie (1 eksabajt = 1 miliard gigabajtów). Z tego 35 procent będzie przenoszone właśnie za pośrednictwem sieci 5G.

Kiedy 5G stanie się wszechobecne, większość urządzeń podłączonych do sieci komórkowych nie będzie już urządzeniami mobilnymi. Mamy tu na myśli urządzenia Internetu Rzeczy takie jak sprzęt gospodarstwa domowego, żarówki, a nawet autonomiczne samochody. Niektóre z nich będą tak potężne, jak urządzenia mobilne, podczas gdy inne będą miały minimalne możliwości obliczeniowe i komunikacyjne. Biorąc pod uwagę różnorodność urządzeń IoT, ich różne możliwości i środowiska wdrożeniowe, wymagania dotyczące ich zabezpieczenia będą wyjątkowo zróżnicowane.

Rok 2024 jest już bardzo blisko. Już teraz należy skupić się na wypracowaniu odpowiednich metod zabezpieczania dużo bardziej zróżnicowanych infrastruktur. Od czego zacząć. Od odpowiedzi na trzy stosunkowo proste pytania: jakie zadanie spełnia dane urządzenie (kontekst aplikacji), z jakimi zagrożeniami możesz mieć do czynienie oraz kto i w jaki sposób może zaatakować. Większa ilość i zróżnicowanie urządzeń niesie ze sobą jeszcze jeden problem. Będzie trzeba stworzyć nowe rozwiązania zabezpieczające dla każdego konkretnego typu aplikacji IoT.

Ograniczenia zasobów niektórych urządzeń IoT również stanowi wyzwanie dla cyberbezpieczeństwa. Wiele istniejących rozwiązań nie jesteśmy w stanie wdrożyć np. w przypadku kamery monitoringu zamontowanej na miejskiej latarni. Ma ona zbyt ograniczone możliwości zarówno obliczeniowe jak i przechowywania danych. Co z urządzeniami IoT bez interfejsu użytkownika? W jaki sposób przeprowadzić autoryzację?

Sieć 5G została stworzona i ustandaryzowana wraz z architekturą sieciową, aby sprostać trzem oczekiwaniom. Ulepszyć mobilną łączność szerokopasmową, komunikację machine-to-machine oraz komunikację o krytycznie niskim opóźnieniu. Dodatkowo, 5G dzięki wdrożeniu nowych protokołów jest znacznie bezpieczniejsza. Zmiany obejmują m.in. ulepszenia w zakresie szyfrowania, wzajemnego uwierzytelniania, ochrony integralności, prywatności i dostępności.

Technologia bezprzewodowa 5G znacznie różni się od wcześniejszych generacji. Należy się liczyć z tym, że wystąpią zupełnie nowe wektory i drogi ataku. Co może stanowić zagrożenie dla sieci 5G? Sieci autonomiczne 5G obsługują radiowe sieci dostępowe 5G (RAN) i zaawansowane EPC (Evolved Packet Cores) - 4G LTE lub LTE. Zagrożenia oraz luki występujące w LTE będą więc również groźne w przypadku 5G NSA. Z jakimi zagrożeniami należy się liczyć?

- Ataki skutkujące wymuszonym przełączeniem się z LTE do 2G/3G, które są dużo mniej bezpieczne.
- IMSI tracking prowadzący do naruszeń w zakresie poufności informacji i prywatności użytkowników.
- Atak man-in-the-middle zagrażający bezpieczeństwu komunikacji serwer-UE (user equipment).
- Ataki cross-protocol - LTE roaming uzależniony od SS7 i protokołu Diameter.
- Bezpieczeństwo i niezawodność to ważne elementy sukcesu tej technologii, a wyzwaniem jest zrozumienie obszaru zagrożeń, które rosną wraz ze wzrostem złożoności sieci.

Urządzenia IoT otaczają nas z każdej strony stanowiąc pożyteczny element funkcjonowania przedsiębiorstw oraz gospodarstw domowych.

Wykorzystanie w procesie produkcji sztucznej inteligencji czy też klasycznych algorytmów pozwala na zwiększenie efektywności funkcjonowania firmy. Na podstawie zagregowanych danych - czy dotyczących przemieszczania się pracowników czy też stanu urządzeń produkcyjnych - możliwe jest przewidywanie wystąpienia awarii oraz optymalizacja wielu procesów produkcyjnych.

Urządzenia IoT, które zagościły w naszych domach, wspomagają nas w codziennych czynnościach. Możemy skonfigurować je w taki sposób, by poranek umilała nam ulubiona muzyka, a tuż po przebudzeniu czekała na nas filiżanka ciepłej, aromatycznej kawy. Co jeszcze? Wraz ze spowolnieniem naszego tętna - które wskazuje na nasze zaśnięcie - zgaśnie telewizor i wygasi się światło.

Niestety, te ułatwienia mają także swoją cenę. Po pierwsze, prywatność użytkownika. Urządzenia Internetu Rzeczy umożliwiają oszacowanie godzin aktywności mieszkańców takiego nowoczesnego domu. W dosyć fatalistycznym scenariuszu pozwalają one na zebranie informacji potrzebnych do bezpiecznego przeprowadzenia... włamania. Dla biznesu rokowania są jeszcze gorsze. Przejęcie kontroli nad urządzeniami produkcyjnymi umożliwia cyberprzestępcom wstrzymanie funkcjonowania firmy, kradzież własności intelektualnej, czy też stary, dobry szantaż.

Głównym wrogiem dla tej kategorii urządzeń jest niewątpliwie ich niska moc obliczeniowa oraz bardzo często spotykany brak możliwości wprowadzania zaawansowych modyfikacji. Uniemożliwia to podjęcie klasycznych kroków zabezpieczających charakterystycznych dla innych endpointów, tj. instalację oprogramowania antywirusowego czy ustawienie zapory ogniowej. Kolejnym utrudnieniem jest mnogość dostępnych mediów/kanałów komunikacji. W przypadku urządzeń IoT może odbywać się ona bezprzewodowo przy pomocy powszechnej sieci komórkowej (2G, 3G, 4G czy 5G), WiFi czy Bluetooth, ale również protokołów dedykowanych dla IoT jak np. ZigBee czy Z-Wave; lub przewodowo przy pomocy sieci Ethernet czy nawet sieci elektrycznej.

Stosunkowo proste do zabezpieczenia są urządzenia IoT opierające komunikację o sieć Ethernet. W ich przypadku możliwe jest wydzielenie części sieci (fizyczne lub wirtualne) dla tego typu urządzeń, a także filtrowanie i monitorowanie przesyłanych danych - z oraz do urządzenia. W przypadku pozostałych metod komunikacji sprawa jest dużo bardziej skomplikowana. Na dzień dzisiejszy - w przypadku każej z nich - znane są metody ataku pozwalające na wymuszenie komunikacji z urządzeniem napastnika. Obecność mostków

pozwalających na wymianę danych pomiędzy sieciami IoT, a LAN wprowadza dodatkowy wektor ataku na sieć komputerową umożliwiając chociażby infekcję urządzeń przy pomocy oprogramowania typu ransomware.

Dlatego konieczne jest ustalenie jakie urządzenia pracują w naszych sieciach wewnętrznych, jakie dane zbierają, w jakiej formie są one później przechowywane oraz przesyłane. Następnym krokiem jest ograniczenie komunikacji wyłącznie do zakresu wymaganego do poprawnej pracy urządzenia, a także monitorowanie przesyłanych danych w celu wychwycenia niestandardowego zachowania.

Nawet zapewnienie tak wysokiego stopnia zabezpieczeń nie daje stuprocentowej pewności co do bezpieczeństwa tego typu urządzeń. Spora część urządzeń Internetu Rzeczy to efekt kompromisu producentów - chodzi w szczególności o ich stopień zabezpieczeń, wydajność oraz, co naturalne, energooszczędność.

Administratorom pracy nie ułatwia fakt, że w dużej mierze mówimy o urządzeniach typu black-box. Wiemy jakiego protokołu na pewno się spodziewać, ale nie mamy pewności czy w ramach układu SoC nie znajdują się inne, niewykorzystywane metody komunikacji pozwalające na dalszą propagację ataku.

Nie należy z tego powodu popadać w paranoję. Podobnie jak w przypadku wszystkich pozostałych urządzeń z którymi obcujemy na co dzień, jedyną pewną metodą zabezpieczenia jest odłączenie zasilania oraz ukrycie urządzeń w klatce Faradaya. Należy pamiętać o standardowych procedurach bezpieczeństwa - ustalaniu potencjalnych wektorów ataku, ograniczaniu prawdopodobieństwa jego wystąpienia oraz niwelowanie jego negatywnych skutków.

Dawid Lewandowski
System Architect, Xopero Software

Cloud Computing
- od chmury nie ma odwrotu

Przyszłość oparta na chmurze to trend, który kształtuje się już od kilku lat. Coraz więcej przedsiębiorstw migruje w kierunku zdalnej infrastruktury. Zarządzanie migracją do chmury wydaje się być niezmiennie jednym z głównych priorytetów firm. Co za tym idzie, rośnie ilość usług dostarczanych w tym modelu. W 2021 roku możemy spodziewać wręcz chmurowego boomu.

Przedsiębiorstwa skłania ku chmurze zwiększona wydajność, szybkość wdrożenia, skalowalność, autonomiczność oraz wspomniana ogólna dostępność rozwiązań zaspokajających wszelkie potrzeby biznesowe. Dodatkowo, co znalazło szczególne zastosowanie w 2020 roku i wybuchu pandemii - daje pracownikom możliwość dostępu do materiałów i programów z dowolnego miejsca i sprzętu, o każdej porze.

Adopcja chmury

Adopcja chmury jest już na wysokim poziomie, ale nie zwalnia tempa - firmy przeznaczają na nią ⅓ swoich inwestycji w IT. Szacuje się, że organizacje przechowują w niej już 46% swoich zasobów, a 95% firm zakłada, że wartość ta wzrośnie do 65% w perspektywie najbliższych dwóch lat. Ten rozwój najszybciej następuje w branżach technologicznej, mediach oraz telekomunikacji, co raczej nie jest zaskoczeniem. Geograficznie przodują tu Stany Zjednoczone. W Europie są to Wielka Brytania, Niemcy i Skandynawia.

Dlaczego firmy decydują się na chmurę?

Z badań przeprowadzonych przez **Microsoft** wynika, że:

- 94% firm z sektora MŚP odnotowuje wzrost bezpieczeństwa po przeniesieniu danych do chmury,
- 59% tych firm zgłasza znaczące korzyści w zakresie wydajności IT, w porównaniu do 30% tych, które nie są jeszcze w chmurze,
- 82% małych i średnich firm informuje o obniżeniu kosztów w wyniku zastosowania technologii chmurowych.
- 70% ponownie inwestuje zaoszczędzone pieniądze w swoją działalność.

Jeżeli chodzi o rozwiązania cyberbezpieczeństwa oparte na chmurze, za ich wyborem przemawia szybszy czas wdrożenia (41%), oszczędność kosztów (41%) oraz ograniczenie działań związanych z dbałością o aktualizacje i wdrażanie poprawek (40%) - tak wynika z **badań CheckPoint**. Dla większości przedsiębiorstw istotna jest również przejrzystość działań użytkowników i zachowania systemu (35%) oraz zdalny dostęp z dowolnego miejsca (35%).

Pomimo znacznych korzyści oferowanych przez rozwiązanie oparte o chmurę, przedsiębiorcy wciąż dostrzegają bariery jej adopcji. Wyzwaniem okazuje się tutaj nie technologia, ale budżet, pracownicy i procesy. Z badań Xopero Software wynika, że dla 51,4% przedsiębiorstw największym wyzwaniem dla

zapewnienia bezpieczeństwa w chmurze są ograniczenia budżetowe. Według blisko 43% firm barierą jest również brak przejrzystości rozwiązań chmurowych. Problemem jest także brak znajomości modeli współdzielonej odpowiedzialności dostawców chmurowych (28,3%) oraz niedostateczna ilość specjalistów security w firmach (27,9%).

Prognozy wartości rynku usług chmury obliczeniowej

Źródło: 300Research

Gartner

214,3 mld USD
2019
331,2 mld USD
2022

IDC

210 mld USD
2019
370 mld USD
2022

ReportLinker

272 mld USD
2019
623,3 mld USD
2023

Chmura publiczna czy prywatna - oto jest pytanie

Niedawne badania pokazują, że firmy balansują pomiędzy chmurą publiczną, a prywatną. Ciężko wyłonić tu zdecydowanego faworyta. Najczęściej bowiem przedsiębiorstwa przechowują swoje zasoby w obu tych modelach jednocześnie.

Czym się różnią? Przede wszystkim chmura publiczna odnosi się do modelu, w którym usługi świadczone są przez internet przez zewnętrznych dostawców infrastruktury. Chmura prywatna jest zaprojektowana specjalnie dla pojedynczej organizacji. Różnica ogranicza się więc do kwestii własności infrastruktury, odpowiedzialności i kontroli.

W ostatnich latach chmury publiczne rosły zdecydowanie szybciej od prywatnych. Dopiero od niedawna możemy zaobserwować odwrócenie tego trendu. Firmy przeznaczają coraz więcej na inwestycje w rozwiązania private cloud. Tempo rozwoju chmur publicznych spadło o niemal 10%, podczas gdy wzrosty w chmurach prywatnych utrzymują poziom powyżej 30%. Wynika to z faktu, że firmy zaczynają szukać bardziej dostosowanych pod ich potrzeby rozwiązań, nad którymi będą mieć większą kontrolę.

Za chmurą publiczną opowiadają się większe przedsiębiorstwa, dla których kwestia odpowiedzialności wymaga bardziej złożonych procesów. Chmura publiczna automatyzuje im proces kontroli i bezpieczeństwa. Przedsiębiorstwa, które mają wyższy stopień adopcji chmury zaczynają jednak skłaniać się ku chmurze prywatnej.

Multi-cloud

Niezaprzeczalnym trendem w 2020 roku będzie rozwój praktyk multicloud. Odnosi się ona do korzystania z wielu heterogenicznych dostawców usług w chmurze, w tym Amazon Web Services (AWS), Google Cloud Platform, Microsoft Azure czy Oracle Cloud, a także platformy jako usługi (PaaS), infrastruktury jako usługi (IaaS) czy dostawców oprogramowania jako usługi (SaaS). Multicloud obejmuje także korzystanie z prywatnych środowisk chmurowych i hybrydowych środowisk chmurowych, które wykorzystują więcej niż jedną publiczną platformę chmurową. Trend ten wynika głównie z chęci dywersyfikacji i rozmaitych ofert dostawców rozwiązań w chmurze, ale także - bezpieczeństwa.

Według raportu RightScale State of The Cloud 2020 by Flexera aż 93% firm decyduje się na wiele rozwiązań chmurowych (multicloud). Średnio używają oni po 2,2 publiczne i 2,2 prywatne chmury oraz eksperymentują z kolejnymi. To znaczący wzrost w stosunku do zeszłego roku, w którym mówiliśmy o 61% przedsiębiorstw.

Niezaprzeczalny wpływ na rozwój praktyk multicloud miał wpływ wybuch pandemii. Ponad połowa respondentów twierdzi, że w najbliższym czasie wykorzystanie chmury będzie wyższe, niż planowano. Inne firmy przyspieszą migrację do chmury ze względu na przejście na model pracy zdalnej i łatwość dostępu do danych. To z kolei pociągnie za sobą wzrost zapotrzebowania na rozwiązania zabezpieczające dane w chmurze i gwarantujące ciągłość działania w momencie wystąpienia awarii.

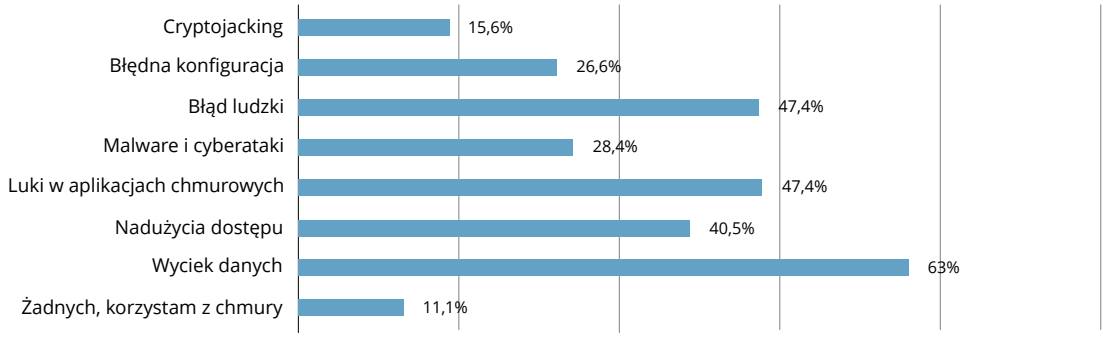
Cloud Threats

Na pytanie o największe zagrożenia bezpieczeństwa, przed którymi stoją infrastruktury chmurowe, organizacje wymieniają wyciek danych (62,8%), luki w aplikacjach chmurowych (47,9%), błędy ludzkie (47,6%), nadużycia dostępu (40,3%) oraz błędną konfigurację - misconfiguration (26,9%).

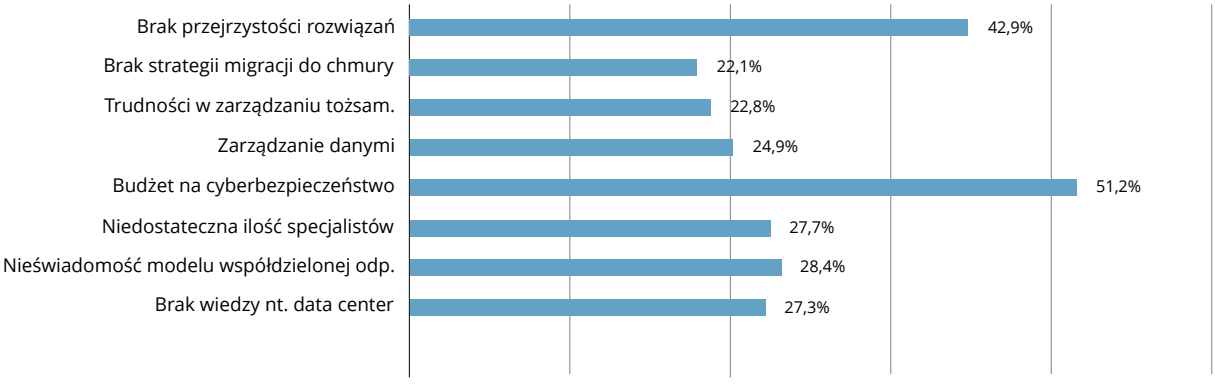
Dokładając do tego cyberataki, takie jak DoS i cryptojacking, oraz niezrozumienie zasad shared responsibility wyznawanych przez większość dostawców chmurowych, jawi nam się całkiem bogaty horyzont problemów i zagrożeń.

Możemy jednak zauważyć, że część tych zagrożeń jest dość ogólna - nie odnosi się wyłącznie do chmury. Wydaje się więc, że obawy związane z transformacją chmurową wynikają z niedostatecznego poziomu świadomości i wiedzy na jej temat lub zagrożeń ogółem.

Jakich zagrożeń w chmurze obawiasz się najbardziej?
Źródło: Xopero Software



Co uważasz za największe wyzwania do zapewnienia bezpieczeństwa w chmurze?
Źródło: Xopero Software



Warto zwrócić uwagę na fakt, że według większości specjalistów infrastruktura cloudowa jest o wiele bezpieczniejsza, niż ta lokalna, stworzona wewnętrznie przez firmę. Wynika to głównie z ilości personelu ds. bezpieczeństwa oraz zasobów i technologii, do których mają dostęp dostawcy chmur publicznych. Niestety, w wielu przypadkach korzystanie z rozwiązań cloudowych wymusza konfigurację po stronie firm-użytkowników - i to właśnie tu najczęściej pojawiają się błędy.

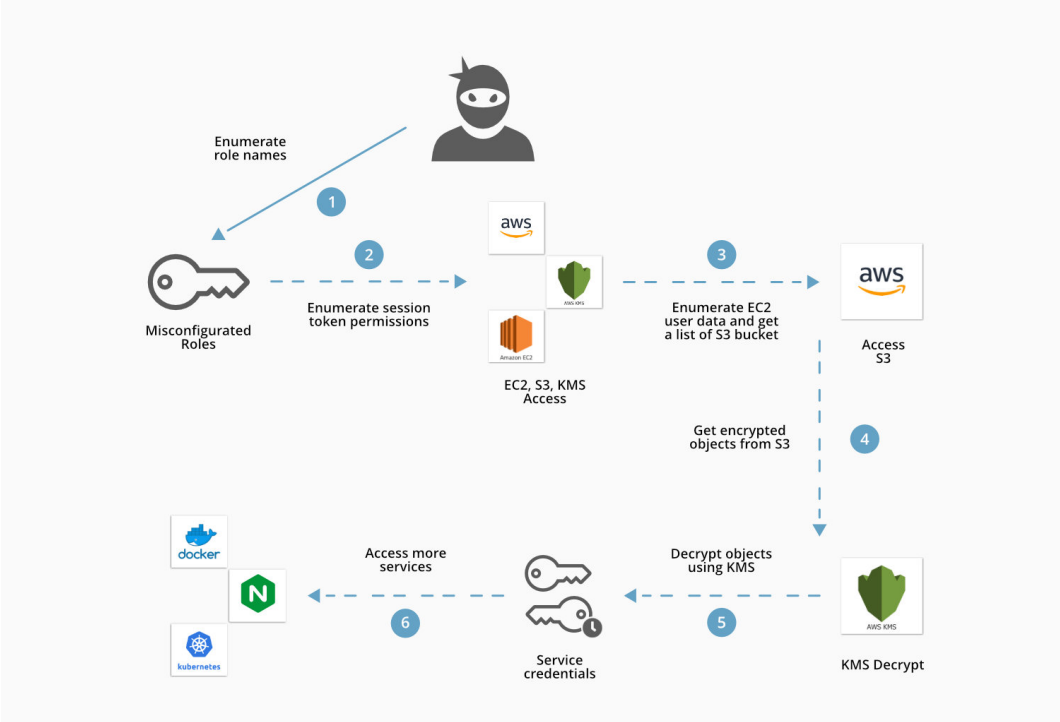
Według Gartnera, jeżeli mowa o bezpieczeństwie w chmurze, to do 2022 roku co najmniej 95% awarii będzie efektem błędów człowieka i organizacji.

Błędna konfiguracja chmury

Błędna konfiguracja i złe zarządzanie zasobami chmurowymi, pozostają najbardziej znaczącym zagrożeniem dla ekosystemu chmurowego. To właśnie te czynniki odpowiadały za szeroką gamę ataków i liczne incydenty kradzieży danych w minionych latach.

Poważne konsekwencje niesie za sobą błędna konfiguracja polityki zarządzania tożsamością i dostępem - IAM (Identity and Access Management) - zarówno po stronie dostawców, jak i użytkowników. IAM to jedna z najbardziej złożonych architektur AWS, Azure i innych usług chmurowych. To za jej pomocą kontrolowany jest dostęp do konkretnych zasobów w ramach chmury. Najczęstszymi błędami, które mogą się tu pojawić są: brak MFA, słabe hasła, brak rotacji haseł co 90 dni, przypisanie wszystkich uprawnień wszystkim użytkownikom zamiast stosowania się do zasady najmniejszego uprzywilejowania, przypisywanie polityki IAM do użytkowników, a nie do grup czy ról. Szczególnie ryzykowne jest nadawanie uprawnień na wysokim poziomie każdemu. Dzięki temu zdobywając klucze, atakujący mogą przeprowadzić niemal każdy atak, kraść wrażliwe informacje, wyczyścić całą infrastrukturę lub zaszyfrować ją z ransomware.

Przykład - na poniższym obrazku widać schemat, za pomocą którego specjaliści z Unit 42 na zlecenie klienta odkryli, wykorzystali i ostatecznie uzyskali dostęp do poświadczeń w środowisku chmurowym



Źródło: **Cloud Threat Report 2H 2020**, Palo Alto Networks&Unit 42

AWS klienta za pomocą błędnie skonfigurowanych ról - przewidywalnych, łatwych do odkrycia z wykorzystaniem enumeracji.

Cryptojacking - chmura koparką walut

Oprócz kradzieży informacji, osoby atakujące celowo nadużywają różnych technologii chmurowych ze względu na ich moc obliczeniową. Od 2019 roku nasilają się kampanie cryptojackingu (złośliwego wydobywania walut) w chmurze czy nadużywanie narażonych hostów Docker / Kubernetes. Szacuje się, że to zagrożenie dotknęło już 23% organizacji, które utrzymują infrastrukturę chmurową.

Najczęściej atakowane są infrastruktury chmurowe w Stanach Zjednoczonych (69%), a jeśli chodzi o Europę - w Niderlandach (11%) i w Niemczech (8%). Wynika to z faktu, że większość węzłów Monero zlokalizowanych jest właśnie w USA.

CENTRUM BEZPIECZEŃSTWA
XOPERO

Cyberataki, malware, luki i podatności - gorące newsy ze świata IT w każdy poniedziałek na Twojej skrzynce mailowej. **Zapisz się!**

Graboid, czyli Docker na celowniku cyberprzestępców
Robak kopiący kryptowaluty wykrada przy okazji dane uwierzytelniające AWS
Microsoft 365: Phishing z OAuth2 w tle / Niespodziewana przerwa w dostępności usług
Przestępcy wykorzystują legalne narzędzie do przejęcia kontroli nad Docker i Kubernetes

Shared responsibility - niezrozumiała kwestia odpowiedzialności

Większość dostawców usług chmurowych (wliczając w to Amazon, Microsoft, Google, IBM, Salesforce, GitHub czy Atlassian) działa w oparciu o tzw. shared responsibility model, czyli koncept współdzielonej odpowiedzialności za kwestie bezpieczeństwa. Użytkownicy usług chmurowych najczęściej wychodzą z założenia, że to dostawcy ponoszą pełną odpowiedzialność za ich ochronę. Tymczasem dostawcy odpowiadają głównie za zapewnienie bezpieczeństwa i dostępności infrastruktury, oprogramowania oraz danych, które wspierają i umożliwiają świadczenie usług, ale to użytkownicy ponoszą odpowiedzialność za bezpieczeństwo przechowywanych w ramach tych usług danych biznesowych. Sami więc muszą zadbać o takie rozwiązania jak backup i disaster recovery, DLP czy EDR. W skrócie: dostawcy są odpowiedzialni za bezpieczeństwo CHMURY, a użytkownicy za bezpieczeństwo W CHMURZE.

Potwierdzają to badania Xopero Software, według których, 71% przedsiębiorców nie ma świadomości istnienia tych modeli i nie jest w stanie w oczywisty sposób określić granicy odpowiedzialności dostawców usług chmurowych od ich własnych obowiązków w zakresie utrzymania bezpieczeństwa IT. W efekcie zaledwie 36% firm przyznaje, że jest w stanie zapobiec utracie danych w chmurze i jedynie 33% kontroluje sposób, w jaki użytkownicy współpracują i udostępniają dane w aplikacjach cloudowych - wynika z raportu McAfee.

To stwarza nie tylko realne problemy organizacyjne, ale stanowi również furtkę dla cyberprzestępców.

Cloud Security

Generalnie środowiska chmurowe uznaje się za bardziej bezpieczne niż infrastruktury lokalne. Wyspecjalizowane centra danych posiadają kilka geograficznych lokalizacji, niezależne linie zasilania, UPS, agregaty prądotwórcze, ochronę fizyczną i całodobowy monitoring systemów, niezbędną certyfikację, detektory dymu i systemy wczesnego gaszenia. Niektóre wyposażone są w biometryczną

weryfikację dostępu. Posiadają również zespół wysoko wykwalifikowanych specjalistów ds. bezpieczeństwa. To wszystko sprawia, że firmie samodzielnie trudniej jest zapewnić taki poziom zabezpieczenia własnej infrastruktury. Ponadto, umożliwia im chociaż częściowe wypełnienie braków kadrowych w zespołach security oraz budżetowych.

IAM - najlepsze praktyki

Jednym z bardziej krytycznych aspektów bezpieczeństwa chmury, o które muszą zadbać działy security IT i DevOps jest odpowiednie zarządzanie polityką tożsamości i dostępu (IAM). Pojedynczy dostawcy chmury zapewniają podstawy do wdrożenia skutecznej polityki dostępu zgodnej z zasadą najniższych przywilejów - czyli oddawania dostępu wyłącznie do tych informacji i zasobów, które są niezbędne do wykonywania określonych zadań. Problem może jednak pojawić się w momencie, w którym firmy korzystają z wielu platform, aplikacji i infrastruktur chmurowych, w których uprawnienia pojedynczego użytkownika będą musiały się różnić - a jak już wiemy dzieje się tak w zdecydowanej większości przedsiębiorstw. Zespoły ds. bezpieczeństwa powinny zatem przygotować kompleksową strategię IAM uwzględniającą potrzeby każdego użytkownika w zakresie wszystkich wykorzystywanych usług cloudowych pamiętając o następujących aspektach:

1. Minimalne przyznawanie uprawnień administratora
2. Korzystanie z opcji przypisywania uprawnień do grup lub ról dla kilku osób pracujących nad jednym projektem (oraz nadawanie rolom nietendencyjnych nazw)
3. Zastosowanie polityki silnych haseł i zmiana haseł/tokenów maksymalnie co 90 dni
4. Wprowadzenie uwierzytelnienia wieloskładnikowego (Multi-factor Authentication, **MFA**)
5. Większe wykorzystanie platform cloud-native security

CASB - chmurowy standard

Jednym z podstawowych zabezpieczeń infrastruktur cloudowych są tzw. wielowęzłowe brokery zabezpieczeń dostępu do usług chmurowych (CASB - Cloud Access Security Broker). Są to nowe technologie bezpieczeństwa, które uzupełniają zapory Next-Generation Firewalls (NGFW), DLP, DPI i inne. Rozwiązują problemy, które pojawiają się przy udostępnianiu danych poza siedzibę firmy. Dają wgląd w to, jakie dane opuszczają firmową sieć, kto je przesyła i w jakie miejsca. Konfiguracja może uniemożliwiać opuszczenie firmowej sieci dla konkretnych danych lub zezwalać na przesyłanie ich do odpowiednich formatów (tokeny, szyfrowanie) i do określonych miejsc docelowych. CASB oferują administratorom większą kontrolę nad danymi, które są udostępniane poza wewnętrzną sieć, konsolidację zabezpieczeń, poprawę zgodności z przepisami związanymi z przetwarzaniem danych w chmurze oraz spójne zarządzanie dostępem i tożsamością. Obecnie stosowane są głównie przez duże przedsiębiorstwa (ok. 64%), ale coraz chętniej sięga po nie sektor MŚP.

Cryptojacking - jak mu zapobiec?

Ochrona przed cryptojackingiem powinna również rozpocząć się od wdrożenia dobrych praktyk w zakresie tożsamości i dostępu. Zagrożenie to stale ewoluuje i poza prostymi operacjami wydobywania kryptowalut może skanować, wykrywać proxy oraz atakować serwery C&C. Robaki mogą łatwo zmienić swoje przeznaczenie i służyć atakom ransomware, eksfiltracji danych. Praktyki, które powinna stosować firma to:

1. Uwierzytelnić wszystkie połączenia kontenera i demona Dockera.
2. Domyślnie blokować wszystkie porty zapory sieciowej
3. Zastosować zasady **NIST SP 800-190** (Application Container Security Guide)
4. Przeglądać ruch sieciowy pod kątem potencjalnych połączeń z mining pools.

Dane są przetwarzane w chmurze. Czyli gdzie? Według GUS dla ponad 30% przedsiębiorców niepewność co do lokalizacji danych jest jednym z głównych powodów, dla którego nie korzystają z chmury.

Nadchodzący rok ma szansę poważnie pobudzić adopcję chmury w Polsce. Zapowiedzi Microsoft i Google już się materializują, a w 2021 roku doczekamy się w Polsce pierwszego regionu globalnej chmury publicznej. Chmura stanie się nie tylko bliższa geograficznie. Tak duże inwestycje branżowych potentatów przyczyniają się do wzmożonego zainteresowania, a w konsekwencji bliższego poznania cloud computing'u. A to brak wiedzy jest największym wrogiem migracji do chmury.

Jak na posunięcie Microsoft i Google zareagują lokalni dostawcy usług chmurowych? Również otwierają kolejne centra danych. W 2021 roku będziemy mieli prawdziwy wysyp nowych obiektów Data Center w Polsce. Na początku roku Netia otworzy DC Jawczyce i będzie to kolejna lokalizacja dla jej usługi chmurowej- Netia Compute, oraz dla innych form outsourcingu infrastruktury IT. Następnie nowe obiekty otworzy między innymi T-Mobile, Orange i ATM. Każde z tych Data Center będzie wykonane na najwyższych światowym poziomie i będzie stanowiło solidny fundament bezpieczeństwa dla świadczonych w nich usług chmurowych. Jest jeden trend, który można dostrzec w większości z nich. Certyfikacja. Do niedawna certyfikowane obiekty w Polsce można było policzyć na palcach jednej ręki. Obecnie prawie każdy nowy obiekt będzie posiadał certyfikat. Pewną nowością jest również wybór samego certyfikatu. Początkowo w Polsce najpopularniejsze były certyfikaty od Uptime Institute (TIER III, IV) lub ANSI/TIA- 942 (Rated 3, 4). Teraz na popularności zyskuje norma EN 50600. Widać to nie tylko u różnych dostawców, którzy chcą posiadać poświadczenie zgodności z tą normą, ale również coraz częściej jest o niej mowa w oficjalnych dokumentach KNF i wymaganiach sektora publicznego. W mojej ocenie w najbliższym czasie będzie to wiodący standard rynkowy.

Jeśli miałbym wymienić tylko jedną usługę, która w 2021 roku ma szansę stać się wspólnym trendem dla chmury i cyberbezpieczeństwa wskazałbym DRaaS. Nie jest to nowy pomysł, ale jego koszty są już na tyle niskie, a świadomość w firmach na tyle wysoka, że prognozuję znaczny wzrost popytu na te usługi w Polsce. Przyczyni się do tego również łatwość budowy hybrydowego środowiska między klientem i dostawcą, gdzie zasoby obu stron często są oparte o wspólną technologię VMware.

W 2021 roku skutki pandemii będą dotkliwiej odczuwalne. Brak środków na zakup sprzętu, szukanie oszczędności, czy potrzeba szybkiego dostosowania się do nowych warunków - to wszystko spowoduje, że klienci zaczną częściej szukać rozwiązań w chmurach.

Adam Kowalczyk
Starszy Kierownik Produktu, Netia S.A.

Załogo! Kurs na „Morze Multicloud”!

Bez względu na to czy Ty i Twoja załoga korzystacie już z jakiegoś dostawcy chmurowego, czy dopiero się do tego przymierzacie, to zapewne prędzej lub później digitalizacja Twojej firmy wypłynie na „Morze Multicloud”.

Ale na dobrą sprawę czym jest ten Multicloud? W skrócie to korzystanie z usług chmurowych więcej niż jednego dostawcy, bez względu na to czy są to usługi infrastruktury publicznej, jako IaaS (Infrastructure as a Service), czy to usługi platformowe, jako PaaS (Platform as a Service), a skończywszy na oprogramowaniu jako usługa, czyli SaaS (Software as a Service). Tak! Mając na uwadze ostatnie, czyli SaaS może się okazać, że już jesteście multicloudowi, ale największe korzyści, jeżeli Twoja organizacja ma takie potrzeby, dają wszelakie mieszanki pomiędzy IaaS i PaaS. I jasno też trzeba podkreślić, że nie dla każdego w obecnej chwili to jedyna i słuszna droga, ale jak wspomniałem na początku, wraz z rozwojem Twojej firmy, oraz rozwojem i dostępem nowych usług chmurowych na rynku, każdy raczej będzie miał z tym do czynienia. Kompletnie bym zapomniał o tym, że szczególną odmianą strategii multicloud jest strategia hybrydowa, gdzie wraz z korzystaniem z zewnętrznych usług cloud Twoja organizacja korzysta z wewnętrznych usług IT, na tych samych zasadach jak z usług dostawców zewnętrznych.

Przed wskazaniem zalet, których jest niemało, muszę lojalnie wspomnieć o wyzwaniach jakie niesie ze sobą multicloud, czyli to na co powinno się zwrócić uwagę.

Po pierwsze, po drugie i po trzecie ... bezpieczeństwo.

Wszystkie modele chmury są podatne na zagrożenia. Bezpieczeństwo w chmurze obejmuje procedury i technologie, które zabezpieczają środowiska chmurowe zarówno przed zewnętrznymi, jak i wewnętrznymi zagrożeniami cyberbezpieczeństwa. Organizacje potrzebują pełnego zaufania do swoich zabezpieczeń w chmurze oraz tego, że wszystkie dane, systemy i aplikacje u dostawców chmurowych są chronione przed wyciekiem danych, kradzieżą, uszkodzeniem i usunięciem. W celu zabezpieczenia środowisk wielochmurowych weź pod uwagę takie potrzeby jak kontrola danych (klasyfikacja, zapobieganie utracie, szyfrowanie), bezpieczny dostęp oraz zarządzanie tożsamością.

Lecz nie (tylko) bezpieczeństwem firmy żyją. Dodatkowo trzeba będzie zdecydować, który z naszych dostawców ma być tym głównym. Dlatego musisz postawić na takiego, który zaleca najlepsze praktyki w zakresie projektowania i obsługi topologii chmury zapewniając maksymalną wartość biznesową ... oczywiście równolegle dbając o najwyższe standardy

bezpieczeństwa.

Najlepsze praktyki zorganizowane są w ramach następujących celów biznesowych:

- bezpieczeństwo i zgodność: zabezpiecz i chroń swoje systemy i zasoby informacyjne w chmurze,
- niezawodność i odporność: twórz niezawodne aplikacje, tworząc odporną infrastrukturę chmury,
- optymalizacja wydajności i kosztów: efektywnie wykorzystuj zasoby infrastruktury i uzyskaj najlepszą wydajność przy najniższych kosztach,
- efektywność operacyjna: aby zapewnić maksymalną wartość biznesową, obsługuj i monitoruj swoje aplikacje oraz zasoby infrastruktury.

Czas na zalety!

Organizacje przyjmują strategię multicloud, aby uzyskać następujące korzyści:

- ekonomia: wybór spośród różnych dostawców usług w chmurze pozwala klientom obniżyć koszty i zoptymalizować ogólne wydatki na IT,
- możliwości: gdy przedsiębiorstwa będą rozwijać różne potrzeby, prawdopodobnie odkryją różnice w ofertach chmurowych,
- dostępność: osadzenie aplikacji na platformach wielu dostawców usług w chmurze zapewnia większą dostępność i odporność na awarie.

Oczywiście powyżej wspomniałem w telegraficznym skrócie o głównych wyzwaniach i zaletach multicloud, co może być dla Ciebie odniesieniem względem pomysłu na budowę jego fundamentów. Uważam, że takie podejście zapewnia wiele korzyści organizacjom, które chcą stosować strategię multicloud, chcą zdecydować się na wybór głównego dostawcy usług chmurowych i chcą ograniczyć ryzyko i wyzwania, które pojawiają się podczas konfigurowania i zarządzania środowiskami multicloud.

Jakub Madej
Cloud Platform and Technology Senior Sales Executive, Oracle

Przyszłość rozwoju w chmurze. Dlaczego przedsiębiorstwa powinny zdecydować się na działanie w modelu chmurowym? Jakie systemy warto w pierwszej kolejności zmigrować?

Nie warto wdrażać rozwiązań chmurowych na siłę. Ten proces powinien być możliwie wszechstronnie przeanalizowany przez pryzmat ryzyk i określenie konkretnych, oczekiwanych kryteriów sukcesu. Przeniesienie do chmury niesie ze sobą wyzwania związane z regulacjami prawnymi, bezpieczeństwem czy dostępem do kompetencji. Uwzględnienie tych czynników może powstrzymywać podjęcie decyzji o przeniesieniu organizacji czy wybranych systemów do rozwiązań chmurowych, ale może także tę decyzję przyspieszyć.

Wiele aplikacji nie jest w 100 proc. zgodnych z modelem chmurowym, w związku z czym naturalne jest migrowanie w pierwszej kolejności mniej krytycznych systemów oraz takich, które z perspektywy organizacji są do tego lepiej przygotowane. Istotne jest, aby organizacja typowała takie systemy bardzo skrupulatnie, - czy to samodzielnie, czy przy wsparciu partnerów technologicznych. Aktualnie mamy do czynienia z nową płaszczyznę konkurencji wśród dostawców usług technologicznych, chmurowych. Usługi świadczone przez największych dostawców i integratorów, opierają się głównie na aspekcie innowacyjności oraz time to market, a nie – jak to było do niedawna, na kwestiach cen.

Takie podejście sprawia, że w rozwiązaniach chmurowych można wdrożyć nowe usługi, aplikacje, systemy i obudować nimi swój core biznes, co daje firmom szanse na konkurowanie z innymi podmiotami na rynku. Potencjał usług chmurowych - w opiniach naszych klientów płynie z jakości usług, kwestii zabezpieczenia danych, automatyzacji mechanizmów deployowania systemów, środowisk i bezpieczeństwa infrastruktury, które łącznie zapewniają ciągłość usług dla biznesu.

Marcin Lebiecki
Dyrektor Zarządzający Cloud and Data Center Department, Asseco Data Systems

„Bezpieczne przejście do chmury czyli wyzwanie dla uporządkowania bezpieczeństwa w organizacji."

Podstawowe pytanie: „W jakiej perspektywie czasowej przenieść usługi do chmury", przestało mieć znaczenie. Według najnowszych badań, większość firm znacznie przyśpieszyła proces migracji i obecnie jest to perspektywa raczej miesięcy niż lat. Pandemia Covid-19, która wymusiła zmianę planów i niekonwencjonalne działania związane z obsługą milionów pracowników podczas pracy zdalnej, wymusiła również zmiany w obsłudze procesów firmowych w innym zdalnym wymiarze. Cyfryzacja postępuje bardzo szybko a pandemia wyzwoliła jego przyspieszenie o około 4 do 6 lat.

Czy dalej istnieją wątpliwości związane z bezpieczeństwem infrastruktury chmury czy bardziej z bezpieczeństwem jej używania w organizacjach - bo to dwa różne aspekty?

Szacunki badaczy mówią, że do 2023 r. użytkownicy chmury w firmach, będą odpowiedzialni za 99% wszystkich incydentów związanych z bezpieczeństwem w wyniku błędów ludzkich, niewiedzy lub niefrasobliwości.

Oznacza to, że jedną z zasad jest współodpowiedzialność dostawcy i klienta za bezpieczne wdrożenie i funkcjonowanie chmury w firmach. Linia demarkacyjna przebiega pomiędzy bezpieczeństwem infrastruktury będącej w jurysdykcji dostawcy a zapewnieniem ochrony danych i aplikacji uruchomionych w chmurze, za które odpowiedzialny jest klient.

Podejście do wdrożenia chmury powinno być świadome a co za tym idzie nawet jeśli szybkie to jednak przemyślane i zaplanowane. Proces wdrożenia chmury będzie prostszy, jeżeli w firmie istnieje tradycja związana z budowaniem procesów, również z perspektywy bezpieczeństwa. Niestety doświadczenie podpowiada, że w tym obszarze jest jeszcze bardzo dużo do zrobienia - również w Polsce. Warto w wziąć pod uwagę „dobre praktyki" publikowane zarówno przez dostawców jak i instytucje związane z bezpieczeństwem posiadające odpowiednie know-how.

Pierwszym z zadań powinna być klasyfikacja oceny informacji i analiza ryzyka ich przetwarzania w chmurze. Pozwoli to na świadomą ocenę tego, co będziemy w chmurze przetwarzać i jak przygotować do tego procesy cyberbezpieczeństwa.

W kolejnym kroku ustalmy kto odpowiada za politykę przetwarzania w chmurze? A w konsekwencji wskażmy właściciela tego procesu i przypiszemy mu tą odpowiedzialność. Skutkuje to konkretnymi ustaleniami i wskazówkami dla użytkowników oraz przygotowaniem procesu zabezpieczenia danych w infrastrukturze chmurowej oraz

sposobu zarządzania aktywami w ramach tego środowiska.

Dalej musi nastąpić stałe zwiększanie kompetencji pracowników i administratorów po stronie klienta. Z jednej strony muszą to być szkolenia czysto techniczne - jak używać „chmury" ale z drugiej szkolenia uświadamiające o zagrożeniach, które mogą być udziałem użytkowników chmury.

Następnie należy ustalić plan bezpiecznego przetwarzania informacji dla chmury oraz ustalić zasady szyfrowania, kontroli dostępu oraz monitoringu całości infrastruktury. W tym miejscu warto zastanowić się czy możemy włączyć te działania do dotychczas wypracowanych procesów (o ile takie mamy) czy też należy stworzyć nowe a być może rozłożyć tą odpowiedzialność - w szczególności za np. doradztwo, szkolenia, monitoring - na zewnętrzne podmioty wyspecjalizowane w tego rodzaju działalności.

Kluczowe jest zawarcie dobrej umowy z dostawcą chmury, która powinna umożliwiać wdrożenie zaplanowanych działań związanych z bezpieczeństwem oraz uwzględniać możliwość realizacji planów ciągłości działania.

Wdrożenie chmury w organizacji będzie bezpieczne o ile przygotujemy się i poświęcimy temu działaniu odpowiednio ukierunkowaną uwagę.

Wojciech Wrzesień
Head of Product Management Team, NASK S.A.

Andrzej Rosłonek
Head of Security Services Department, NASK S.A.

Machine Learning
a cyberbezpieczeństwo, szanse i zagrożenia

Gdzie kończy się prawda a zaczyna hype?

Uczenie maszynowe niewątpliwie odegra istotną rolę w stworzeniu nowej klasy rozwiązań dla specjalistów od cyberbezpieczeństwa. Nowa technologia już dziś znajduje zastosowanie m.in. w wykrywaniu zagrożeń, zautomatyzowanej analizie sieci, wyszukiwania wzorców, skanowaniu skrzynek mailowych czy jako wsparcie w threat hunting. Wielu dziennikarzy wysuwa śmiałą tezę, że AI będzie/jest naszym cyber-zbawcą. W rzeczywistości, czasy Neo jeszcze nie nadeszły. Pytanie, czy kiedykolwiek nastaną?

Należy postawić jasną granicę oddzielającą realne możliwości uczenia maszynowego od odwiecznego marzenia, o stworzeniu maszyny myślącej w sposób do tej pory możliwy wyłącznie dla istot ludzkich. Zwłasza, że Biznes jest dziś pełen paradoksów. Z raportu opracowanego przez **Webroot** czytamy, że 96% respondentów korzysta z rozwiązań cybersecurity, które posiadają moduły AI. To znacznie więcej niż dwa lata temu. Według danych zebranych przez **Capgemini w roku 2018**, 28% ankietowanych korzystało z rozwiązań, które posiadają wbudowane moduły AI, a 30% z własnych wypracowanych algorytmów. Wróćmy teraz do współczesności. Paradoksalnie pomimo zdecydowanego wzrostu ilości adopcji, ponad połowa managerów nie do końca rozumie, jaką wartość AI wnosi do obszaru bezpieczeństwa. A w szczególności, czy w przypadku ich organizacji jest ona w stanie efektywnie radzić sobie z wyzwaniami które stoją na co dzień przed działem IT. Na koniec, 70% badanych zamierza wdrażać tego typu mechanizmy w większej skali... Pomimo faktu, że nie rozumieją ich realnej wartości i nie wiedzą jak przekłada się ich stosowanie na utrzymanie infrastruktury bezpieczną. Marketing odgrywa w tym całkiem sporą rolę.

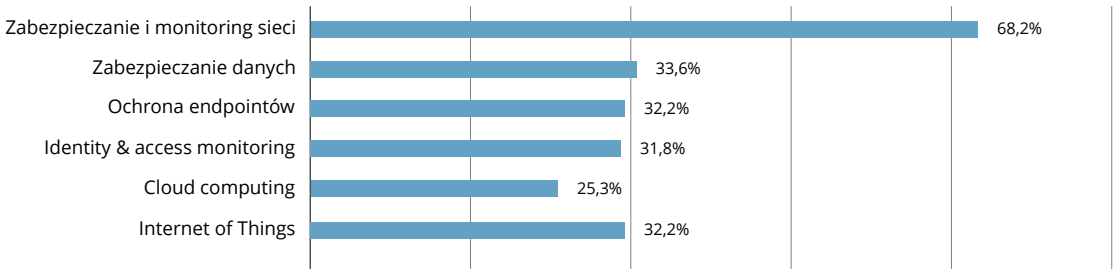
Jak na tle tych badań wypada Polska? Administratorzy oraz specjaliści ds. bezpieczeństwa największe szanse w wykorzystaniu uczenia maszynowego dostrzegają w rozwiązaniach umożliwiających zabezpieczenie oraz monitoring sieci. Tego zdania jest ponad 68 procent ankietowanych. Jednak nie jest to jedyny obszar, który czerpie korzyści z wykorzystania danej technologii. Ponad 33 procent respondentów uważa, że AI ma również wpływ na zabezpieczenie danych. Kolejne 32 procent głosów przypadło na ochronę endpointów. Podobne wnioski wynikają z licznych zagranicznych raportów.

Z jakich rozwiązań wyposażonych w moduł lub moduły uczenia maszynowego korzystają jednak w praktyce specjaliści? Najwięcej osób – ponad 66 procent – wskazuje na rozwiązania typu antywirus oraz antymalware. 42 procent głosów przypada na filtry antyspamowe. Tylko 26 procent respondentów stwierdziło, że nie korzysta z żadnego rozwiązania tego typu.

Z danych zebranych w czasie badania wynika również, że około 30 procent ankietowanych posiada jedno lub więcej wdrożonych rozwiązań ML. 13 procent jest obecnie na etapie testów, a 14 procent zabezpieczyło na ten cel środki w budżecie na rok 2021. Ponad 42 procent ankietowanych nie planuje jednak

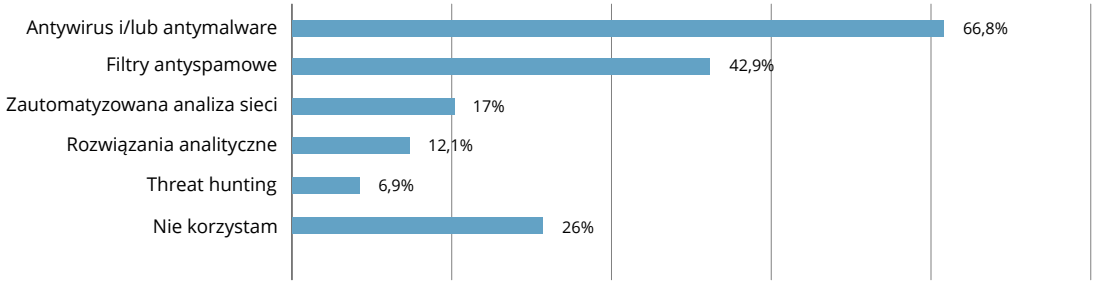
W jakich obszarach cyberbezpieczeństwa uczenie maszynowe znajduje największe zastosowanie?

Źródło: Xopero Software



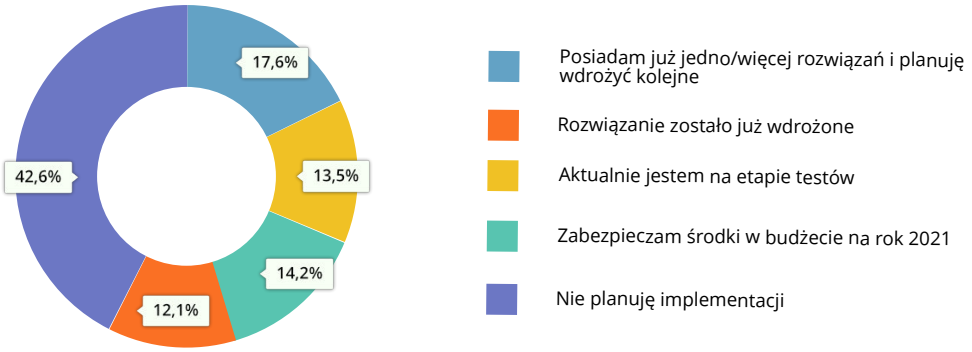
W jakich rozwiązań cybersecurity wyposażonych w moduł uczenia maszynowego korzystasz?

Źródło: Xopero Software



Na jakim etapie wdrożenia rozwiązań machine learning obecnie się znajdujesz?

Źródło: Xopero Software



implementacji takiego rozwiązania w swojej organizacji.

Skoro większość ankietowanych dostrzega praktyczne zastosowanie dla uczenia maszynowego, nasuwa się pytanie: dlaczego nie planują wdrożeń? Wiele z dostępnych obecnie na rynku rozwiązań jest dedykowana dla firm z obszaru enterprise. Wolniejsze tempo wdrożeń to być może skutek niedostosowania produktów do wymogów IT polskich podmiotów, a także stosunkowo wysoki koszt zakupu takiego rozwiązania. Pomimo to, zapotrzebowanie na tego typu usługi w MŚP jak najbardziej występuje - mamy więc do czynienia z niszą na rynku, która zapewne bardzo szybko się zapełni.

Algorytmy wbudowane w produkty z obszaru bezpieczeństwa IT można co najwyżej określić mianem słabego lub wąskiego AI. Dlaczego? Wykonują one wysoce wyspecjalizowane zadania w ramach jednej (wąskiej) dziedziny. Dalej, zostały przeszkolone w oparciu o zbiór big data, specyficzny dla tego właśnie konkretnego obszaru. Jest to dalekie od ogólnej (lub silnej) sztucznej inteligencji, która w założeniu powinna być systemem będącym w stanie wykonywać dowolne uogólnione zadanie i odpowiadać na pytania w wielu domenach. Obecnie dostępne na rynku rozwiązania, są bardzo dalekie od tego.

Przyjrzyjmy się detekcji anomalii. Anomalie to zdarzenia odbiegające od wartości typowej lub średniej. Z uwagi na trudność w definiowaniu zdarzeń normalnych, anomalie wykrywane przez systemy mogą czasami być obarczone błędami – alertami fałszywie pozytywnymi oraz fałszywie negatywnymi. Duża liczba fałszywych alertów psuje integralność systemu i wpływa na pogorszenie wyników detekcji. Dlatego to człowiek jest nadal integralnym elementem, decydującym o sukcesie wdrożenia takich rozwiązań. Bo to ostatecznie specjaliści IT decydują, które alerty stanowią informację o realnym zagrożeniu. Jednak im więcej fałszywie dodatnich wyników generuje algorytm, tym więcej zdarzeń będzie musiał przeanalizować zespół.

Rozważmy teraz następującą sytuację. W jaki sposób dzisiejsza (a nawet jutrzejsza) sztuczna inteligencja może odróżnić intruza z niebezpiecznymi zamiarami od osoby technicznej, która może wykonywać dane operacje? Jak odróżnić chodzenie w sposób pewny od podejrzanego? Jak ma tego dokonać algorytm? Uczenie maszynowe może oferować imponujące możliwości, które mogą strategicznie uzupełniać pracę już wykonywaną przez zespoły ds. bezpieczeństwa - ale żaden z nich nie może zastąpić ludzkich członków tych zespołów. Sztuczna inteligencja zapewnia wysoki poziom precyzji i specjalizacji, podczas gdy ludzie mają zdrowy rozsądek i kontekstową wiedzę. Człowiek i maszyna muszą się wzajemnie uzupełniać, aby działać efektywnie. Firmy zajmujące się bezpieczeństwem, które chcą wykorzystać sztuczną inteligencję, muszą uznać realistyczne możliwości tej technologii.

Wielu nietechnicznych obserwatorów uważa dziś sztuczną inteligencję za technologię science fiction o wydajności na poziomie ludzkiego mózgu. W rzeczywistości sztuczna inteligencja jest tak inteligentna, jak dane, które dostarczają jej badacze. Zamiast zakładać, że niezdolność sztucznej inteligencji do wykonywania określonych zadań jest porażką samej technologii, konsumenci muszą pogodzić się z faktem, że właśnie taką sztuczną inteligencją dziś dysponujemy. Powinniśmy skupić się na realnych możliwościach technologii - i właśnie jej realne możliwości zamierzamy zaprezentować w kolejnym podrozdziale.

Cyberbezpieczeństwo w dobie AI

W jaki sposób uczenie maszynowe może zmienić obecnie wykorzystywane przez atakujących techniki wdzierania się do sieci, czy infiltrację systemów ofiary?

Badaczy szczególnie interesuje stopień w jakim uczenie maszynowe może wpłynąć na rozwój obecnie stosowanych strategii kill chain. Mamy tu na myśli sekwencje działań, które hakerzy podejmują, aby osiągnąć swoje cele – naruszyć infrastrukturę, wykraść dane uwierzytelniające itp.

Czy uczenie maszynowe może zostać wykorzystane do wynajdywania luk w oprogramowaniu? Zautomatyzowane skrypty już teraz wspomagają wykrywanie podatności, które potencjalnie mogą posłużyć do cyberataku. Narzędzia typu fuzzers dostarczają specjalnie opracowane inputy, które mają za zadanie wywołać awarię, która z kolei ma ujawnić potencjalną podatność lub błąd w kodzie.

Czy systemy uczenia maszynowego mogą wspomóc przeprowadzanie ataków typu spearphishing? Dziś jest to jedna z najbardziej powszechnych i skutecznych technik ofensywnych. Jeśli systemy uczenia maszynowego mogą generować wiarygodne komunikaty, które wydają się pochodzić od wiarygodnych nadawców - i są w stanie uniknąć wszelkich zautomatyzowanych prób wykrycia - mogą znacznie przechylić szalę sukcesów na stronę atakujących. Wydaje się to mało prawdopodobne? Generator języka OpenAI o nazwie GTP3, samodzielnie stworzył spójny artykuł, opublikowany na łamach The Guardian. O czym właściwie „pisał" program? O tym, jak to jest być robotem. W kontekście tych odkryć, napisanie przez algorytm maila do naszego współpracownika może więc być dziecinnie proste.

Czy uczenie maszynowe może wpłynąć na skuteczność rozprzestrzeniania się złośliwego kodu? Możliwości samo-rozprzestrzeniania się złośliwego kodu (self-propagating) są już znane od kilkudziesięciu lat. Wspomnijmy chociażby robaka Morris'a z 1988 roku. Zautomatyzowany mechanizm propagacji NotPetya - który opierał się głównie na kradzieży haseł, ale także na exploicie opracowanym przez amerykańskie NSA – umożliwił rozprzestrzenianie się zagrożenia w ramach infekowanej sieci w dosłownie kilka minut. Biorąc pod uwagę, jak imponujące mogą być zwyczajne mechanizmy propagacji – bez wykorzystania sztucznej inteligencji – należy postawić już teraz pytanie, w jakim stopniu algorytmy usprawnią takie ataki w przyszłości.

Kolejna kwestia warta rozważenia to ukrywanie obecności oraz Anti-Forensics. Czy uczenie maszynowe może lepiej ukryć ofensywne operacje cybernetyczne? Jednym z głównych celów intruzów jest uniknięcie złapania. Jeśli uczenie maszynowe wspomaga zespół ds. bezpieczeństwa, trzeba założyć, że może wspomóc również hackerów w pozostaniu niezauważonym.

W jaki sposób systemy uczenia maszynowego mogą pomóc w wykrywaniu włamań i reagowaniu na nie, a także w usuwaniu szkodliwego kodu?

Wiążemy wielkie nadzieje z wykorzystaniem uczenia maszynowego do wzmocnienia cyberochrony. Dziś spore wyzwanie stanowi wykrywanie przeciwnika w ramach własnej sieci. Czas namierzania intruzów jest ściśle uzależniony od stopnia wyrafinowania stosowanych przez nich technik. Niestety średnio jest to ponad 1 rok. I chociaż tempo wykrywania tego typu ataków ciągle się poprawia, wielu intruzów ukrywa się w firmowej sieci przez długie miesiące. Jeśli uczenie maszynowe może usprawnić wykrywalność takich zdarzeń, ich powstrzymywanie lub atrybucję, może to radykalnie zmniejszyć potencjalne zagrożenia związane z operacjami cybernetycznymi.

Czy machine learning może pomóc we wczesnym wykrywaniu złośliwego kodu w ramach sieci lub systemu operacyjnego? Wykrywalność zagrożeń jest fundamentalnym wyzwaniem dla cyberobrony. Jeśli przeciwnik nie zostanie znaleziony, nie można go usunąć. Wiele ataków cybernetycznych przebiega bez przeszkód przez długie miesiące lub lata. Właśnie z powodu niepowodzenia w ich wykrywaniu. Uczenie maszynowe może znacznie poprawić nasze wyniki w tym zakresie. Szczególnie, że ilość danych w ramach sieci jest tak ogromna, że większość technik innych niż sztuczna inteligencja, w tym analiza ludzka, zwyczajnie nie nadąża. Podczas gdy ludzie nadal muszą badać i rozstrzygać o bardziej złożonych alertach, systemy uczenia maszynowego mogą weryfikować ogromne zbiory danych w celu wykrycia anomalii.

Czy uczenie maszynowe może pomóc powstrzymać, a nie tylko wykryć, ofensywne operacje cybernetyczne? Jest zrozumiałe, że jeśli uczenie maszynowe może wykryć działania ofensywne, prawdopodobnie może również pomóc w opóźnieniu lub ich zablokowaniu. Czyli mówimy tutaj o rozszerzeniu modułów wykrywania o obronę, powstrzymywanie ataków a nawet ingerencję w złośliwe operacje.

Czy w systemach uczenia maszynowego mogą występować podatności – w algorytmach lub też danych, od których są uzależnione ich wyniki?

Czy systemy uczenia maszynowego można oszukać i czy można je zabezpieczyć przed takimi próbami oszustwa? Jednym z podstawowych zadań współczesnego uczenia maszynowego jest klasyfikacja: określenie, do której kategorii coś pasuje. Na rynku ta technika znalazła bardzo wiele zastosowań - od filtrów antyspamowych, po narzędzia do rozpoznawania obiektów. Każdy dobry system klasyfikacji musi być wyczulony na fałszerstwa, kamuflaż i oszustwa. Czwórka może wyglądać bardziej jak dziewiątka, a spam może brzmieć autorytatywnie i wiarygodnie. Wszystkie te metody wykorzystują sposób w jaki ludzki mózg przetwarza informacje. Jednak w błąd można wprowadzać również algorytmy. Adversarial Machine Learning jest właśnie tego przykładem. Na czym polega ta taktyka? Atakujący uderzają w mechanizmy używane przez sieci neuronowe do przetwarzania informacji i dokonywania klasyfikacji. Hakerzy mogą stworzyć zbiór danych – obrazów png, które dla człowieka wygląda zupełnie zwyczajnie, jednak dla maszyny już nie. Zmiana na poziomie kilku pikseli może radykalnie wpłynąć na wynik pracy algorytmu. Co ważniejsze, w sposób prawie całkowicie niewykrywalny dla ludzkich obserwatorów.

Czy systemy uczenia maszynowego mogą zawieść z powodu problemu z danymi w oparciu o które są trenowane? W tym wypadku szczególnie interesujące mogą okazać się próby zatrucia danych, czyli metoda o nazwie Data Poisoning. Dobór danych oraz ich jakość ma fundamentalne znaczenie we wszystkich operacjach z wykorzystaniem inteligentnych algorytmów. Dla hakerów może więc stanowić niepowtarzalną okazję do zmylenia programów. Podmiana danych w oparciu o które system się uczy, może diametralnie odmienić sposób w jaki będzie się on później zachowywał. Jest to szczególnie niebezpieczne w sytuacji gdy mamy do czynienia z systemami, które uczą się w oparciu o dane typu input – czyli dane generowanych przez samych użytkowników. Głównie chodzi w tym przypadku o systemy rekomendacji i niektóre filtry antyspamowe.

Podczas gdy atak z wykorzystaniem data poisoning koncentruje się na zanieczyszczaniu procesu uczenia klasyfikatorów sieci neuronowych, równie groźne mogą być ingerencje w dane typu input. Mowa tu o ataku o nazwie Data Pipeline Manipulation. Nieodpowiednie zabezpieczenia lub ich całkowity brak mogą pozwolić cyberprzestępcom na modyfikowanie danych wejściowych podczas ich przesyłania albo kiedy są przechowywane na serwerach. Atakujący mogą na przykład zmodyfikować skany CT, gdy dane będą przesyłane ze skanera CT na serwer danych. W sytuacji gdy urządzenie ma nieaktualne oprogramowanie lub niezabezpieczone porty zwykła podatność może stać się furtką dla atakujących.

Sposób na niedostateczne zbiory danych

AI stwarza dziś spore możliwości, jednak uczenie maszynowe zwykle wymaga bardzo dużej ilości danych. Niestety badania pokazują, że prawie połowa firm wskazuje, że jest to największe wyzwanie podczas implementacji AI. Tylko 54% ankietowanych posiada odpowiednie zbiory danych. Nie chodzi wyłącznie o brak odpowiedniego zbioru big data. Problemy pojawiają się także podczas integracji rozwiązania z infrastrukturą IT, wykorzystywanymi systemami danych oraz aplikacjami. Kolejnym wyzwaniem jest płynna aktualizacja danych, w oparciu o które pracują algorytmy. Od tych czynników zależy sukces implementacji AI w firmie. Model trenowany w oparciu o niezrównoważony zbiór, daje zawsze niezadowalające efekty. W takim razie, czy algorytmy mogą uczyć się efektywniej w oparciu o mniejsze zbiory danych?

Aby model AI był w stanie rozpoznać konia, specjalista musi najpierw pokazać mu tysiące obrazów tego zwierzęcia. Sposób w jaki programy uczą się i poznają świat jest całkowicie odmienny od ludzkiej percepcji i sposobu uczenia właściwego dla ludzi. Dziecko zazwyczaj potrzebuje zaledwie kilka przykładów zdjęć lub obiektów aby z sukcesem rozpoznawać je w przyszłości. Ale to nie wszystko. W szczególnych sytuacjach dziecko nie potrzebuje żadnych fizycznych

przykładów obiektu, aby zidentyfikować go w późniejszym czasie. Jeśli pokażemy mu zdjęcie konia a potem nosorożca oraz zaznaczymy, że jednorożec jest czymś pośrednim będzie ono w stanie zidentyfikować go w książce z bajkami. Niewiele uwagi poświęcamy swojej własnej umiejętności percepcji, a jest ona naprawdę niezwykła. Czy jednak algorytmy mogą poznawać w podobny sposób?

I tak, i nie. Percepcja inteligentnych algorytmów jest zupełnie odmienna od ludzkiej. Jednak najnowsze badania sugerują, że modele AI również powinny być w stanie wykonać podobne operacje. Specjaliści z Uniwersytetu w Waterloo (Kanada) nazwali ten proces nauki „Less than one". U jego podstaw leży założenie, że model sztucznej inteligencji powinien być w stanie dokładnie rozpoznać więcej obiektów niż liczba przykładów, na których został przeszkolony. Badacze przetestowali swoją teorię w oparciu o popularny zbiór danych, który służy do prac nad computer vision. Baza MNIST zawiera 60 tys. obrazów przedstawiających ręcznie zapisane cyfry w przedziale od 0 do 9. Wracając do samej techniki – na czym ona dokładnie polega? Kiedy pomyślimy o cyfrze „3", to w pewnym sensie wygląda ona trochę jak „8" jednak nie przypomina w ogóle „7". Zamiast więc mówić maszynie, „To jest cyfra 3" naukowcy proponują komunikat „Ten obraz jest w 60 procentach cyfrą 3, w 30 procentach cyfrą 8 i w 10 procentach cyfrą 0". Jeśli „Less than one" okaże się sukcesem, pozwoli to drastycznie zredukować wymogi dotyczące zbiorów danych – ich woluminu i jakości. W ten sposób sztuczna inteligencja stałaby się także dużo bardziej dostępna dla firm i branż, które do tej pory były ograniczane przez wymagania dotyczące big data.

PUŁAPKI

„Magia" nowych technologii – coś jest, ale go nie ma, chociaż jest...

Absurdalny tytuł? Trafny w kontekście tego, o czym za chwilę przeczytacie. Czy czerwona czapka może być triggerem umożliwiającym zniknięcie obiektu? Okazuje się, że może. Naukowcy wykazali, że kamera YOLO (popularne na rynku kamery do wykrywania obiektów) była w stanie początkowo wykryć obiekt, jednak jeśli posiadał on na głowie czerwoną czapkę – pozostawał niezauważony. Bardzo podobny test – w którym wzięły udział dwie osoby ubrane w podobny t-shirt różniący się wyłącznie kolorem – dał zbliżone rezultaty. Obie osoby nie zostały wykryte przez kamerę.

Problem ze sztuczną inteligencją, pomimo jej skuteczności i zdolności rozpoznawania tak wielu rzeczy, jest taki, że jest ona z natury podatna na błędy. W przypadku tradycyjnego programu przeprowadzamy jego testy, staramy się wywołać potencjalne błędy itd. W skrócie – jesteśmy w stanie bardzo dokładnie zweryfikować jak będzie zachowywał się dany kod. Jednak w przypadku uczenia maszynowego, model można testować tylko pod kątem jego użyteczności. Na przykład model, który został zaprojektowany do rozpoznawania obiektów lub klasyfikowania wiadomości e-mail posiada bardzo ograniczony zakres testowania. W sytuacji, kiedy nie zostanie wyszkolony do wykrywania wszystkich możliwych scenariuszy – co z góry jest skazane na porażkę – może on stanowić zagrożenie dla bezpieczeństwa firmy lub innych podmiotów.

Czy AI może paść ofiarą językowych pułapek?

Jak oszukać AI w rozwiązaniach takich jak Siri, czy Alexa? Chociażby poprzez podmianę używanych słów. Oprogramowanie o nazwie TextFooler jest w stanie oszukiwać systemy NLP (natural-language processing) zastępując w zdaniu określone słowa ich synonimami.

Oprogramowanie, opracowane przez zespół z MIT, szuka w zdaniu słów, które są najważniejsze dla klasyfikatora NLP i zastępuje je synonimem, który człowiek uznałby za naturalny. Na przykład zmiana zdania „Postacie obsadzone w niemożliwie wymyślonych sytuacjach są całkowicie oderwane od rzeczywistości" na „Postacie obsadzone w niemożliwie zaaranżowanych okolicznościach są całkowicie oderwane od rzeczywistości" dla nas nie robi w zasadzie żadnej różnicy. Jednak sztuczna inteligencja interpretuje każdy z tych dwóch wariantów w zupełnie inny sposób.

Kiedy Ty to nie Ty na Twoim zdjęciu paszportowym

Zespół specjalistów z firmy McAfee opracował przykładowy atak na systemy rozpoznawania twarzy (facial recognition systems) - bardzo podobne do tych, które na lotniskach wykorzystuje się do weryfikacji paszportów. Z pomocą uczenia maszynowego stworzyli obraz, który dla ludzkiego oka wyglądał jak jedna osoba, jednak przez algorytm brał go za kogoś zupełnie innego. W teorii więc na pokład samolotu mogłaby wejść osoba, która nie znajduje się na liście pasażerów.

Jak dokonano tego oszustwa? Do wprowadzenia w błąd systemu, naukowcy wykorzystali algorytm translacji obrazów znany jako CycleGAN. Z jego pomocą można przekształcać zdjęcie z jednego stylu w inny. Cyfrowe zdjęcie portu może wyglądać tak, jakby było w rzeczywistości obrazem który wyszedł spod pędzla Moneta. Inny przykład – zdjęcie gór latem, można przekształcić w taki sposób, że będzie wyglądało tak jakby zostało zrobione zimą.

Zespół McAfee wykorzystał 1500 zdjęć każdego z dwóch obiektów i wprowadził je do CycleGAN, aby przekształcić je jeden w drugi. Po wygenerowaniu setek obrazów, CycleGAN ostatecznie stworzył sfałszowany obraz, który gołym okiem wyglądał jak osoba A, ale oszukał system rozpoznawania twarzy, że to jednak osoba B.

Chociaż badanie budzi wyraźne obawy co do bezpieczeństwa systemów rozpoznawania twarzy, istnieją pewne zastrzeżenia. Po pierwsze, naukowcy nie mieli dostępu do rzeczywistego systemu używanego przez lotniska do identyfikacji pasażerów. Zamiast tego skorzystali z najnowocześniejszego algorytmu open source. Po drugie, taki atak wymaga odpowiednich zasobów i sporej ilości czasu. CycleGAN potrzebuje wydajnych komputerów – a atakujący – specjalistycznej wiedzy, jak wyszkolić algorytm.

Edukuj się!

Czy inteligentne algorytmy mają realne przełożenie na cyberbezpieczeństwo? Więcej na ten temat przeczytasz w raporcie **„Machine Learning i cyberbezpieczeństwo”**.

Pobierz

Sztuczna inteligencja to technologia, która jak żadna inna oddziałuje na naszą wyobraźnię. Kino i literatura przez dziesiątki lat dostarczały nam masę materiału, który stał się poniekąd bagażem. Bo kiedy pada dziś hasło „AI" przed oczami maluje się nam obraz miasta z *Łowcy Androidów*, albo HAL z *Odysei Kosmicznej*. Czyli nasze pragnienia, bądź też głęboko skrywane lęki, które jednak odstają od rzeczywistości. Problem z uczeniem maszynowym jest taki, że w warunkach laboratoryjnych działa ono prawie niezawodnie. Za to w momencie zetknięcia z rzeczywistymi danymi, model nie daje już tak dobrych wyników.

Budowanie modelu polega na trenowaniu go w oparciu o dużą liczbę przykładów. Następnie testuje się go w oparciu o kolejny obszerny zbiór danych, z którymi jednak algorytm nie miał jeszcze do czynienia. Kiedy model zalicza test, praca jest skończona. I być może w tym właśnie tkwi problem. Skąd mamy pewność, że otrzymane w ten sposób wyniki są wiarygodne? W środowisku pojawiły się głosy przemawiające za opracowaniem sposobu, dzięki któremu sieć neuronowa może przetwarzać dane oraz generować prognozę i poziom pewności modelu w oparciu o jakość dostępnych danych. Dziś potrzebne są nam modele, które nie tylko wyróżnia wysoka wydajność. Ważniejsze jest by być w stanie szacować, kiedy nie możemy im ufać. Określając niepewność modelu, uzyskujemy także dodatkowe informacje m.in. jakich błędów możemy się spodziewać lub jakie dane mogą wpłynąć na poprawę jego działania. Każda dziedzina wiedzy, która ostatecznie sięgnie po uczenie maszynowe, będzie musiała dysponować również szacunkiem niepewności wyników.

Co ciekawe, uczenie maszynowe może stać się wydajniejsze i dużo bardziej niezawodne, jeśli naśladuje modele biologiczne. Mam tutaj na myśli systemy oparte na mózgach prostych zwierząt. Nowe wyniki badań pokazują, że prostsze, mniejsze sieci neuronowe mogą znaleźć zastosowanie w niektórych typach zadań. Wypadają one znacznie lepiej, działają wydajniej i są bardziej niezawodne niż popularne obecnie algorytmy. Taki nowatorski system jest w stanie m.in. sterować pojazdem za pomocą niewielkiej liczby sztucznych neuronów.

A skoro przytaczam przykad pojazdu mechanicznego, wiele osób zapewne zadaje w myślach pytanie *"Jak się on sprawdził w zetknięciu z „prawdziwymi" danymi?"*. Badania pokazały, że system znacznie lepiej poradził sobie z „hałaśliwymi" danymi wejściowymi, niż obecnie stosowane rozwiązania. Do tego dzięki prostocie, można szczegółowo wyjaśnić jego tryb działania. Nie jest więc on traktowany jak czarna skrzynka, a wręcz przeciwnie - może on być zrozumiany przez ludzi. Z całą pewnością jest to bardzo ciekawa teoria. Tym bardziej, że w ostatnich latach sukcesy na polu uczenia maszynowego były powiązane ze zwiększaniem mocy obliczeniowej. Brakowało trochę świeżości i innowacji. Co w takim razie niesie najbliższa przyszłość? Jednym z niewątliwych kierunków rozwoju będzie upraszczanie złożonych modeli, a także opracowanie nowego rodzaju sieci neuronowych.

Karolina Dzierżyńska
Redaktor Centrum Bezpieczeństwa, Xopero Software

Porównywanie wydajności pracownika InfoSec ze sztuczną inteligencją jest jak porównywanie testów manualnych do automatycznych: z jednej strony jest wykwalifikowany specjalista zdolny do zauważenia niuansów i znający psychologię człowieka, a z drugiej wirtualny robot, zdolny do wykonywania dziesiątek testów na minutę. Niemniej, w ostatnim czasie sztuczna inteligencja zaczyna doganiać kompetencje pracowników nawet w dziedzinach, w których zazwyczaj dominowali ludzie.

Poprzez zbieranie metadanych z różnych źródeł, systemy SIEM wyposażone w AI zaczynają rozumieć mentalność człowieka. Wydajność pracy, opóźnienia, wykorzystywane aplikacje oraz odwiedzane strony internetowe brane są pod uwagę w ocenie ryzyka związanego z zachowaniem użytkownika. Jeżeli sztuczna inteligencja zauważa zachowania typowe dla insidera lub osobę nadużywającą swoich przywilejów, może podjąć natychmiastową reakcję, choćby alertującą lub ograniczającą dostęp do danych.

Ale nie tylko na wczesnym rozpoznawaniu insiderów się kończy. W przeciwieństwie do pracowników, systemy wyposażone w sztuczną inteligencję pracują non-stop, przez co są w stanie reagować na zagrożenia pochodzące z zewnątrz w trybie on-time. W praktyce oznacza to różnicę pomiędzy analizą skutków ataku post-factum, a analizą działań, które sztuczna inteligencja podjęła w imieniu administratora.

W najgorszym wypadku, nawet kiedy de-facto dochodzi do wycieków, sztuczna inteligencja przyczynia się do obniżania kosztów ich wykrywania i reagowania na zaistniałą sytuację. Według danych Capgemini - Reinventing Cybersecurity with Artificial Intelligence, ponad połowa firm (56%) twierdzi, że ich analitycy ds. bezpieczeństwa cybernetycznego są przepracowani, przez co blisko jedna czwarta (23%) nie jest w stanie z powodzeniem zadbać o wszystkie zidentyfikowane incydenty. Niemniej, nawet w takich sytuacjach, używanie sztucznej inteligencji do wykrywania wycieków post-factum przyczynia się do średniego obniżenia kosztów związanych z wyciekiem o 12%.

Niestety, byłoby zbyt dobrze, gdyby nie istniała druga strona medalu. Sztuczna inteligencja jest również wykorzystywana przez cyberprzestępców na coraz większą skalę w celu atakowania firm. W porównaniu do tradycyjnych (manualnych lub zautomatyzowanych) testów penetracyjnych, sztuczna inteligencja może łączyć wiedzę z darknetu oraz różnego rodzaju exploity w jeden, dobrze skoordynowany atak. W takich sytuacjach, paradoksalnie, może pomóc tylko dobry monitoring i szybka reakcja, czyli sztuczna inteligencja w naszej obronie. I tak koło się zamyka.

Paweł Wałuszko
Cybersecurity Expert, TestArmy

Backup i Disaster Recovery

Nowy standard bezpieczeństwa

Dane są siłą napędową każdego biznesu i nierzadko stanowią o ich wartości i wycenie. Umożliwiają firmom nie tylko zarządzanie i rozwój bieżącej działalności, ale napędzają ich rozwój oraz budowanie przewagi rynkowej. Globalnie biznes odpowiada za ok 30% generowanych informacji. Tu pojawia się problem - przy tak dużym sukcesie biznesu opartego na odpowiednio utrzymywanych i dostępnych danych biznesowych, konsekwencje ich utraty nigdy nie były poważniejsze. Firmy muszą więc nie tylko opracowywać strategie ich ochrony, ale zabezpieczyć się na wypadek najgorszego - utraty danych oraz zagrożenia utraty dostępu do krytycznych usług i aplikacji, które nimi operują.

Najprostszym rozwiązaniem jest tutaj backup, czyli regularne tworzenie kopii zapasowych oraz disaster recovery (DR) - zestaw polityk i procedur, których głównym zadaniem jest przywrócenie dostępu do usług, krytycznych dla funkcjonowania biznesu, na wypadek wystąpienia jakiejkolwiek awarii.

Według badań Xopero Software, backup jest drugim, najchętniej wykorzystywanym rozwiązaniem z obszaru IT security i staje się standardem, z którego korzysta 89,6% ankietowanych. Plasuje się tuż za antywirusami i oprogramowaniem anty-malware (94,5%) - które stało się właściwie fundamentem dzisiejszego podejścia do zabezpieczania danych i urządzeń firmowych. Popularność backupu rośnie tym bardziej, że według Ponemon Institute oprogramowanie antywirusowe jest nieskuteczne w przypadku aż 60% ataków.

Należy zwrócić uwagę, że powodów utraty danych z przedsiębiorstw jest wiele - mowa tu nie tylko o atakach cybernetycznych. Może być nim błąd lub lekkomyślność pracownika (co stanowi najczęstszą przyczynę utraty danych i dystrybucji malware), przypadkowe skasowanie danych, awaria sprzętu/systemów, shadow IT, kradzież urządzeń, awarie zasilania czy klęski żywiołowe. Potrzebę świadomego podejścia do kwestii bezpieczeństwa danych zauważają i narzucają również organy prawodawcze - stąd Rozporządzenie o Ochronie Danych Osobowych porządkujące temat przetwarzania danych osobowych i wprowadzające narzędzia do wymierzania odczuwalnych kar finansowych w przypadku naruszeń.

Rynek backupu i disaster recovery

Znaczenie backupu w codziennym funkcjonowaniu przedsiębiorstw będzie przybierać na mocy. Rynek backupu i disaster recovery jest jednym ze stabilniej rozwijających się w branży cybersecurity. **Prognozuje się**, że jego wartość do 2022 roku wyniesie 11,59 mld dolarów przy średniej rocznej stopie wzrostu (CAGR) w wysokości 10,2%. Głównymi czynnikami napędzającymi rozwój tego rynku będzie wspomniana już eksplozja produkowanych danych, rosnąca ilość zagrożeń, coraz większe zainteresowanie procesami zachowania ciągłości działania biznesu i zarządzania danymi. Ogromne (wręcz kluczowe) znaczenie będzie miał tutaj rozwój rynku cloud computingu - zwłaszcza w kontekście przechowywania danych, cloud backupu oraz trendu multicloud. **Szacuje się**, że wartość rynku backupu w chmurze wzrośnie do 10,25 mld dolarów w 2025 roku, przy założeniu średniej rocznej stopy wzrostu (CAGR) na poziomie aż 25,90% (!). Obrazuje to

poniekąd, w jaki sposób będzie rozwijał się rynek backupu ogółem. Skierowanie się firm w kierunku rozwiązań chmurowych to jeden z istotniejszych trendów na nadchodzący rok, również w branży backupu.

Backup w użyciu

Postanowiliśmy sprawdzić, w jaki sposób firmy korzystają z rozwiązań do backupu. Według przeprowadzonych badań, przedsiębiorstwa przeznaczają na takie oprogramowanie do 10% całkowitego budżetu IT. Gdzie przechowują kopie zapasowe? 43% ankietowanych zdecydowało się na rozwiązania hybrydowe (połączenie backupu lokalnego z cloudowym), ponad 37% korzysta wyłącznie z rozwiązań on-premises, a więc przechowuje dane lokalnie, na serwerach w siedzibie firmy. 5,6% postawiło tylko na produkty do backupu chmurowego. 13,4% ankietowanych wciąż zgrywa swoje dane na zewnętrzne dyski.

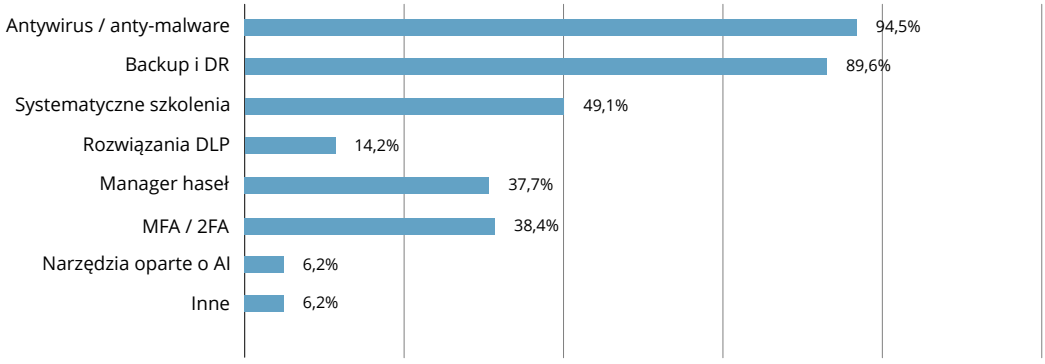
Optymizmem napawają statystyki dotyczące częstotliwości tworzenia kopii zapasowych. Blisko 60% ankietowanych w badaniu Xopero Software deklaruje, że wykonuje backup codziennie. 12,4% robi go nawet częściej - kilka razy dziennie. Raz w tygodniu i częściej - 18,6%. Raz w miesiącu lub rzadziej swoje dane backupuje zaledwie 4,1% przedsiębiorców.

Co zabezpieczają? Bazy danych (74,5%), serwery (68,6%), pojedyncze pliki (63,8%), komputery (53,1%), maszyny wirtualne (50%) oraz w mniejszym stopniu pocztę e-mail (37,9%) i urządzenia mobilne (15,5%).

Cloud backup

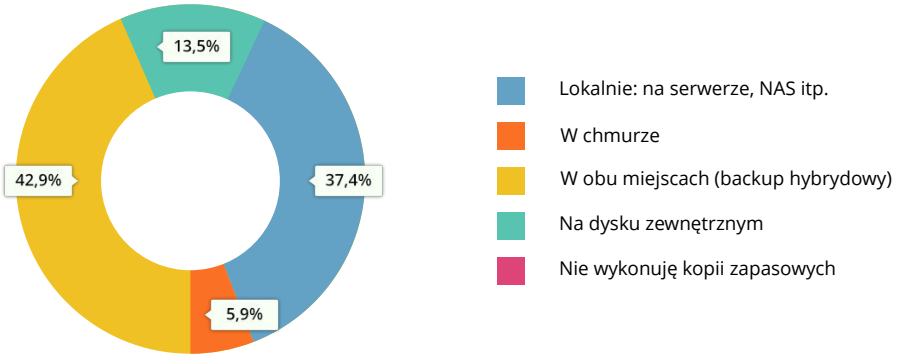
Chmura publiczna wniosła nowy element do branży backupu, zapewniając szybkie odzyskiwanie, centralne zarządzanie, oszczędność kosztów i skuteczny sposób na zapewnienie ciągłości działania. Największy potencjał dostrzegają w niej firmy z sektora MŚP, dla których stworzenie odpowiedniej infrastruktury IT jest ogromnym i często nieopłacalnym przedsięwzięciem. Cloud umożliwia im wyeliminowanie kosztów utrzymania infrastruktury oraz podnosi poziom ochrony danych poprzez przeniesienie ich poza siedzibę firmy i kontrolę przez większą i wyspecjalizowaną kadrę. Za korzystaniem z backupu w chmurze przemawia również trend pracy zdalnej oraz większe użycie urządzeń mobilnych. Proces backupu jest więc uniezależniony od lokalizacji urządzenia, ponieważ wykonuje się automatycznie i zdalnie z wykorzystaniem łącza internetowego.

W jaki sposób zabezpieczasz swoją infrastrukturę IT?
Źródło: Xopero Software



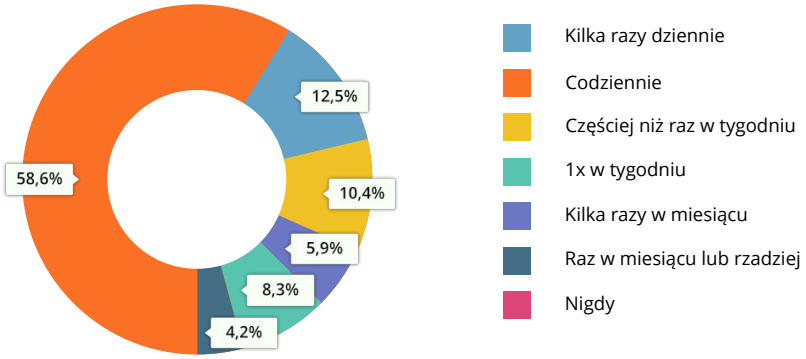
Gdzie przechowujesz swoje kopie zapasowe?

Źródło: Xopero Software



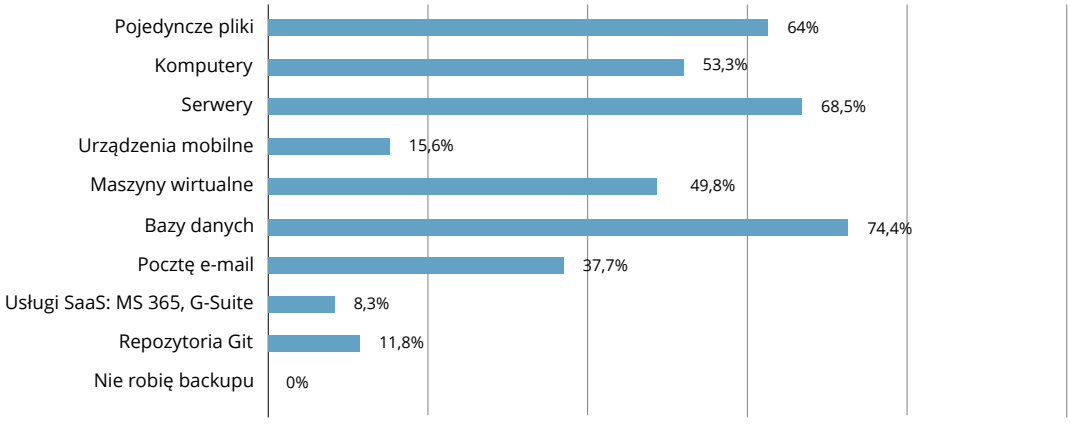
Jak często wykonujesz backup?

Źródło: Xopero Software



Co zabezpieczasz?

Źródło: Xopero Software



Cloud-delivered backup

Jeżeli mowa o cloud backupie, to możliwość zabezpieczenia danych w chmurze - a więc zewnętrznym centrum danych lub tworzenie kopii zapasowych danych przetwarzanych w ramach usług chmurowych to dziś absolutna podstawa. Trendem w ostatnich czasach staje się jednak wykorzystanie chmury w procesie projektowania rozwiązań do backupu. Mowa tu o produktach cloud-delivered security.

Jest to podejście w tworzeniu oprogramowania, które wykorzystuje chmurę do tworzenia i uruchamiania skalowalnych, łatwo zarządzalnych aplikacji w nowoczesnych i dynamicznych środowiskach. Tak tworzona architektura wyróżnia się łatwym zarządzaniem i pełną automatyzacją. Pozwala inżynierom na uproszczone wprowadzanie zmian przy mniejszym wysiłku, a co za tym idzie bardziej płynne i częstsze aktualizacje oraz usprawnienia oprogramowania.

Z punktu widzenia użytkownika cloud-native backup niesie szereg korzyści. Firma nie potrzebuje mieć własnych zasobów i nie ponosi kosztów utrzymania infrastruktury ponieważ serwer zarządzania usługą znajduje się w chmurze. Oczywiście, można postawić go lokalnie - tu decyzja należy już do firmy. Postawienie usługi w chmurze umożliwia łatwą skalowalność rozwiązania i zabezpieczenie nawet najbardziej złożonej i rozproszonej infrastruktury. Odpowiada również na potrzeby łatwego zabezpieczenia danych pracowników mobilnych lub zdalnych.

Serwera zarządzania nie należy mylić z serwerem w ujęciu magazynu danych. Fakt, że usługa postawiona jest w chmurze nie oznacza, że użytkownik musi być ograniczony do storage'u cloudowego. Z punktu widzenia obsługi oprogramowania może nawet nie zauważyć różnicy. Może więc przechowywać kopie zapasowe lokalnie np. na udziałach sieciowych SMB czy lokalnych zasobach dyskowych, w chmurze (np. AWS S3, Azure) lub dowolnej kombinacji tych magazynów (np. backup hybrydowy, multi-cloud).

Cloud-delivered backup umożliwia nie tylko oszczędność zasobów i łatwe zarządzanie, ale również jest rozwiązaniem zapewniającym zdecydowanie wyższy poziom bezpieczeństwa.

Multi-cloud, bo jedna chmura to za mało

W rozdziale poświęconym Cloud Computingowi piszemy o rosnącym znaczeniu praktyk multi-cloud, a więc korzystaniu z wielu heterogenicznych dostawców usług w chmurze. Trend ten został zauważony przez producentów rozwiązań do backupu. W efekcie, co niektórzy umożliwiają wykorzystanie wielu chmur publicznych jako magazynów danych. W ramach jednego rozwiązania i różnych planów można mieć przypisanych wiele magazynów chmurowych, które w dodatku będą się replikować. I tak też przykładowo - dane mogą być przechowywane w Amazon Web Services w Stanach Zjednoczonych oraz replikowane do Microsoft Azure w zupełnie innej lokalizacji geograficznej - np. w jednym z krajów europejskich. Wówczas firma jest w pełni zabezpieczona przed wszelkimi awariami i katastrofami naturalnymi, które mogą spotkać centrum danych w jednej z lokalizacji. W takiej sytuacji organizacja nawet nie odczuje problemu, który dotknął jedno z centrów danych i zachowa ciągłość działania, a w razie potrzeby - przywróci dane z alternatywnej, działałającej chmury.

Firmy będą wybierać rozwiązania do backupu i disaster recovery, które umożliwiają nie tylko przechowywanie kopii w wielu chmurach (a więc dodanie kilku magazynów chmurowych), ale także replikację danych i migrację do innych używanych środowisk. Wybierając podejście multi-cloud w zakresie backupu i zabezpieczenia danych, organizacje zyskują elastyczność, niezależność od dostawcy i niezawodność. Podejście to pozwala bowiem na zwiększenie odporności na awarie, katastrofy oraz ataki na poziomie chmury i wynikającą z tego utratę danych. Przyśpiesza proces odtwarzania danych w przypadku wystąpienia awarii oraz umożliwia zapewnienie zgodności z przepisami

dotyczącymi ochrony danych oraz innymi regulacjami dotyczącymi przetwarzania informacji i prywatności.

SaaS Backup

Jeżeli chodzi o multi-cloud to rozwiązania do backupu powinny nie tylko dać możliwość wykorzystania wielu różnych magazynów danych w chmurze, ale również zapewnić firmom bezpieczeństwo danych w ramach używanych aplikacji chmurowych. Mowa tu chociażby o najbardziej popularnych usługach SaaS (ang. Software-as-a-Service - oprogramowanie jako usługa), a więc Microsoft 365 (dawniej Office 365) czy Google Workspace (dawniej G Suite).

Wielu przedsiębiorców na pytanie o bezpieczeństwo danych w ramach Microsoft 365 odpowiada, że ich dane przechowywane są przez Microsoft, któremu przecież nie zdarzają się awarie czy ataki. Tymczasem, sam gigant technologiczny zaleca stosowanie zewnętrznego oprogramowania do backupu danych i zabezpieczenie informacji przechowywanych w ramach pakietu Microsoft 365. Firma ta, jak i większość dostawców usług SaaS, działa bowiem w oparciu o model współdzielonej odpowiedzialności (ang. shared responsibility model), w ramach którego odpowiedzialny jest za zabezpieczenie i sprawność działania infrastruktury chmurowej. Bezpieczeństwo danych przetwarzanych w ramach ich usług spoczywa jednak na samych użytkownikach - z czego z reguły nie zdają sobie sprawy. Ponadto, bez rozwiązania do backupu danych i disaster recovery, wystarczy nawet krótka przerwa w dostępie do usług Microsoft czy Google, aby firma naraziła się na przestój w działaniu i poważne straty finansowe.

Problemem może okazać się również ograniczona retencja w ramach różnych programów pakietu Microsoft 365, która zazwyczaj wynosi miesiąc. Oznacza to, że dane w koszu przechowywane są przez okres 30 dni, a następnie są usuwane na zawsze i nie ma możliwości ich przywrócenia. Jeżeli użytkownik przypadkowo (lub celowo) usunie plik, folder, maila czy zdarzenie w kalendarzu - będzie w stanie przywrócić je wyłącznie w ciągu 30 dni, w których znajdują się jeszcze w koszu (tzw. soft deletion). Później straci te dane na zawsze (tzw. hard deletion). Przedsiębiorcy poszukujący oprogramowania do backupu Microsoft 365 powinni więc zwracać uwagę na oferowane przez producentów możliwości konfigurowania wersjonowania i retencji oraz upewnić się, że są w stanie ustawić schemat rotacji kopii dokładnie taki, jakiego potrzebują (np. w ramach GFS - Grandfather-Father-Son). Dzięki temu zapewnią pełną kontrolę nad czasem, przez jaki będą przechowywane kopie, oszczędność miejsca na magazynie oraz szybsze przywracanie danych.

Na jeszcze co powinni zwrócić uwagę firmy poszukujące oprogramowania do backupu Office 365? Na kompleksowość rozwiązania (zabezpieczenie poczty mailowej, kalendarza, OneDrive itd.), dowolny storage (możliwość przechowywania kopii w chmurze lub na storage'u lokalnym), automatyzację, zaawansowane wyszukiwanie i granularne odzyskiwanie bezpośrednio na konta użytkowników

CENTRUM BEZPIECZEŃSTWA XOPERO

Cyberataki, malware, luki i podatności - gorące newsy ze świata IT w każdy poniedziałek na Twojej skrzynce mailowej. **Zapisz się!**

Oto incydenty bezpieczeństwa gigantów technologicznych:

Poważny błąd w Microsoft Teams pozwala na atak bez interakcji użytkownika
61% serwerów Microsoft Exchange nadal podatnych na zdalne wykonanie kodu
Microsoft Teams z błędem, który umożliwiał przejęcie konta za pomocą... obrazka .GIF
Awaria Google – Gmail, YouTube, Google Drive i Hangout padły na blisko godzinę

Microsoft 365 lub na własny komputer.

Coraz częściej powstają też programy do backupu ograniczające się do konkretnych branżowych usług SaaS, takich jak systemy CRM (np. Salesforce, ZOHO) czy platformy e-commerce typu Shopify czy Shoper.

Backup lokalny - kierunek: multiplatfomowość

Proces migracji do chmury, choć przybiera tempa nadal nie jest na wystarczająco wysokim poziomie. Firmy wciąż mocniej ufają lokalnej infrastrukturze IT. Z punktu widzenia klienta istotną cechą jest więc kompatybilność rozwiązań do backupu z infrastrukturą lokalną, którą już posiada - zarówno w kontekście zabezpieczenia i backupu, jak i przechowywania danych.

Na poziomie backupu mowa tutaj chociażby o wsparciu dla środowisk fizycznych (endpointów i serwerów) oraz środowisk wirtualnych, które często idą w parze.

Sama usługa backupu powinna być możliwa do zainstalowania lokalnie na wielu systemach wykorzystywanych w ramach organizacji lub obsługiwana jako usługa w chmurze, która nie wymaga instalacji i konieczności utrzymywania dodatkowego sprzętu.

Co z magazynem danych? Według raportu Network Attached Storage (NAS) Market - Growth, Trends, and Forecast blisko 80% średnich i dużych przedsiębiorstw korzysta z rozwiązań typu NAS do przechowywania danych. Tym samym przy wyborze rozwiązania do backupu danych i DR klienci zgłaszają potrzebę kompatybilności oprogramowania z macierzami NAS, z których korzystają. Motywem jest łatwość implementacji oraz ograniczenie kosztów poprzez brak konieczności inwestycji w dodatkową infrastrukturę IT.

Zważając jednak na rosnące wykorzystanie chmury, możemy spodziewać się, że firmy skłonią się ku rozwiązaniom hybrydowym, które pozwolą im zabezpieczyć dane zarówno lokalnie, czy to na serwerze typu NAS czy udziałach sieciowych SMB oraz replikację do magazynów chmurowych.

Disaster Recovery - nie daj się przestojom

Szacuje się, że globalnie średni jednostkowy koszt związany z przestojem działalności firmy wynosi 1,52 mln dolarów! Ta kwota stanowi aż 40% łącznych kosztów incydentu bezpieczeństwa i wycieku danych. Do utraty przychodów z działalności zaliczone zostały skutki utraty klientów, przestojów systemów i rosnące – z powodu strat wizerunkowych – koszty pozyskania nowych źródeł przychodów. Nic dziwnego, że statystycznie 93% firm bez disaster recovery upada w rok po utracie danych.

Według badań Cisco Benchmark Study ok. 40% firm doświadczyło przestojów dłuższych niż 8 godzin z powodu poważnej awarii. 39% podało, że co najmniej połowa ich systemów została dotknięta poważnym naruszeniem.

Plan disaster recovery (Disaster Recovery Plan, DRP) to część planu zachowania ciągłości działania - Business Continuity Plan (BPC). Jest to dokument, który zawiera analizę ryzyka związanego z utratą dostępu do kluczowych usług oraz procedury działania. Podstawą jest tu założenie, że w każdej chwili może dojść do nieprzewidzianej awarii o dużej skali, która może sparaliżować infrastrukturę IT i działanie całej firmy. Ta katastrofa/awaria może wystąpić w wyniku m.in. błędu ludzkiego, przyczyn naturalnych czy cyberataku. Dlatego jeżeli mówimy o zabezpieczeniu infrastruktury, mamy na myśli nie tylko dane, ale również zapewnienie szybkiego, a wręcz natychmiastowego dostępu do wszelkich istotnych usług (np. CRM czy ERP). Plan disaster recovery obejmuje więc planowanie, wdrażanie odpowiedniej technologii i nieustanne testowanie. Należy określić tu m.in. procedury, dokumentację, sprecyzować role pracowników, opisać szczegóły systemu IT czy plan naprawy szkody.

Backup jest tutaj kluczowym elementem. Powinien być zautomatyzowany oraz umożliwiać centralne

zarządzanie i odzyskiwanie danych z i do dowolnej lokalizacji w jak najkrótszym czasie. Jedną z ważniejszych funkcjonalności jest tutaj możliwość uruchamiania krytycznych maszyn (fizycznych i wirtualnych) w zapasowym środowisku wirtualnym. W ten sposób użytkownicy są w stanie szybko przywrócić działanie i dostęp do krytycznych systemów i usług. Ważne jest również, aby po usunięciu awarii można było przywrócić wszystkie zmiany na środowisko produkcyjne.

Do niedawna o procedurach DR mówiono w odniesieniu do dużych systemów informatycznych i telekomunikacyjnych. Przed katastrofami zabezpieczały się głównie banki, instytucje finansowe lub operatorzy telekomunikacyjni. Czyli te podmioty, u których nawet najmniejszy brak dostępu do świadczonych usług mógł wywołać milionowe straty, a nawet kosztować je istnienie. Dziś po DR sięgają małe, średnie i duże firmy. Wynika to nie tylko ze wzrostu świadomości o zagrożeniach, ale także większej dostępności i przystępności samych rozwiązań.

Choć wdrożenie planu odzyskiwania po awarii wymaga poniesienia kosztów na infrastrukturę, administrację i technologię, jest to inwestycja, która zwraca się 4-krotnie. Przyjmuje się bowiem, że każdy 1$ wydany na plan odtwarzania awaryjnego przynosi firmie 4$ oszczędności w momencie jej wystąpienia.

Automatyzacja i UX to podstawa

Badanie przeprowadzone przez firmę Forrester potwierdziło potrzebę automatyzacji procesów backupu i disaster recovery - 34% przedsiębiorstw nadal ma problemy z automatycznym tworzeniem kopii zapasowych i odzyskiwaniem danych. Organizacje stoją w obliczu rosnącej potrzeby korzystania z niej w celu zwiększenia wydajności, monitorowania stanu backupu i zapewnienia ogólnej niezawodności tworzenia kopii zapasowych. Często nie są w stanie określić solidnych, zautomatyzowanych planów tworzenia backupów i mechanizmów odzyskiwania po awarii. Korzystanie z nich ad-hoc jest trudne, zwłaszcza gdy trzeba wykonać kopię zapasową dużych i złożonych środowisk z wieloma wewnętrznymi zależnościami.

Firmy powinny sięgać po rozwiązania, które zapewniają nie tylko automatyzację procesów backupu, ale też centralne zarządzanie, intuicyjną konfigurację, prosty monitoring. Ułatwieniem będą tutaj cykliczne (np. codzienne) raporty ze statystykami tworzenia kopii zapasowych, alertami o niepowodzeniach oraz możliwość testowania kopii i procesów odtwarzania na wypadek faktycznych zdarzeń. Ta ostatnia możliwość jest istotna nie tylko z punktu widzenia sprawdzenia celowości i sprawności samego rozwiązania, ale umożliwia również weryfikację czasu niezbędnego na przywrócenie działania krytycznych systemów oraz określenie statystyk SLA (ang. Service Level Agreement - umowy dotyczącej jakości usług informatycznych).

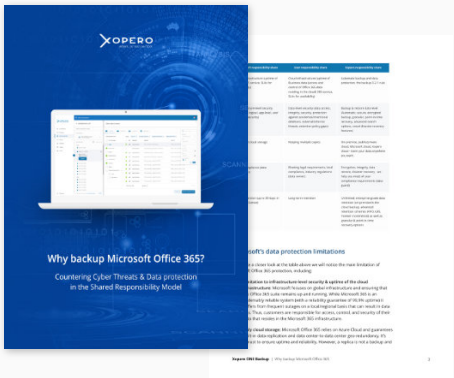
Potrzeby przedsiębiorstw są coraz bardziej złożone. Jednocześnie na rynku wciąż brakuje rozwiązań, które zapewniają funkcjonalności klasy korporacyjnej w sposób i w cenie przystępnej dla małych i średnich przedsiębiorstw. Takie rozwiązania nie tylko zapewniają możliwość zabezpieczenia niemalże dowolnej infrastruktury IT w dowolnej lokalizacji, ale również gwarantują łatwą skalowalność oprogramowania wraz ze wzrostem firmy. Mowa tu m.in. o łatwym dodawaniu kolejnych urządzeń do planów, kolejnych magazynów danych, masowym wdrożeniu, rozłożeniu wykonywania kopii zapasowych w czasie w celu ograniczenia obciążenia łącza i zwiększenia efektywności backupu oraz dowolnych ustawień retencji w zależności od wymagań i potrzeb biznesu - w tym, zaawansowanych schematów typu GFS.

W branży bezpieczeństwa IT mówi się, że ludzie dzielą się na tych, którzy robią kopie zapasowe i tych, którzy dopiero będą je robić. Dziś możemy mówić podobnie w kontekście disaster recovery. Jeszcze do niedawna barierę stanowiły koszty wdrożenia, a często także brak odpowiedniej znajomości rynku i potrzeb związanych z zabezpieczeniem infrastruktury na wypadek awarii. Na szczęście wraz z dostępnością

rozwiązań, rośnie świadomość przedsiębiorstw. Zdecydowana większość podmiotów na rynku posiada już oprogramowanie do backupu i DR. Gartner przewiduje jednak, że do 2022 roku, 40% organizacji zastąpi swoje dotychczasowe rozwiązania do tworzenia kopii zapasowych i odzyskiwania awaryjnego nowymi.

Na co zwrócą uwagę przedsiębiorstwa? W 2021 roku małe i średnie firmy będą poszukiwać produktów, które w sposób płynny i ekonomiczny zapewnią im jak największą ochronę. Z pewnością wybiorą producentów, którzy mogą pochwalić się kompleksową ofertą, skalowalnością, ochroną w modelu SaaS (cloud-native backup), centralnym zarządzaniem, szybkim odzyskiwaniem danych czy obsługą wielu platform.

Poza aspektami funkcjonalnymi, coraz bardziej złożone potrzeby przedsiębiorstw skłaniają ich do poszukiwania intuicyjnych rozwiązań, które w prosty i przystępny sposób pozwolą im zabezpieczyć nawet najbardziej rozbudowaną infrastrukturę IT. Firmy skierują się więc kierunku UX i wyboru prostych konsoli zarządzania, przejrzystych, napędzanych danymi dashboardów, których obsługa nie wymaga zaawansowanych umiejętności IT - jest prosta, łatwa i przyjemna. W dodatku, takie aspekty jak powiadomienia mailowe, statusy wykonania kopii, ostrzeżenia, audyt logów i sprawny support mogą przeważyć o wyborze właściwego oprogramowania.



Edukuj się!

Więcej na temat modelu współdzielonej odpowiedzialności i zagrożeń dla pakietu Microsoft Office 365 znajdziesz w dokumencie **“Why backup Microsoft”**.

Pobierz

Rynek rozwiązań do backupu danych jest bardzo mocno zależny od rozwoju wielu gałęzi informatyki, ale także od innych rynków. Niemal w każdej branży znajdziemy użytkowników tych systemów. Zdecydowanie można powiedzieć, że rok 2020 przyniósł wiele wyzwań dla większości przedsiębiorstw na całym świecie. Pandemia wymusiła na firmach wiele zmian, w tym oczywiście organizacyjnych, a te wpłynęły na sposób przetwarzania oraz przechowywania danych.

Wiele firm zdecydowało się na model pracy zdalnej, pracownicy zaczęli wykonywać swoje codzienne obowiązki z domowego zacisza i tym samym część infrastruktury (np. komputery) została zdecentralizowana. Nie zmieniła się ilość wykorzystywanych i wytwarzanych danych, ale często zmieniła się ich lokalizacja. Znamy wiele przypadków, gdzie pracownicy korzystają z prywatnego sprzętu, na którym zapisują pliki związane ze swoją pracą. Dane te oczywiście trzeba zabezpieczać i to najlepiej w taki sposób, by minimalizować obciążenie łącza internetowego w siedzibie firmy, gdzie zwyczajowo znajdował się magazyn danych, tak by zapewnić prawidłowe działanie VPN, czy innych usług, które pozostały na lokalnych serwerach. Wykonywanie kopii bezpośrednio do chmury to najlepszy sposób, by sprostać temu wyzwaniu i tym samym wśród niektórych systemów dostępnych na rynku pojawiła się możliwość wykonywania kopii do popularnych usług storage w chmurze, najczęściej Amazon AWS oraz Azure. Magazyny chmurowe to również doskonałe miejsce, gdzie możemy replikować nasze kopie przechowywane lokalnie, w myśl zasady 3-2-1. Dobrze jest również mieć możliwość replikowania takich magazynów, czy też wykonywania ich kopii na magazyny lokalne (np. urządzenia NAS) lub przechowywania kopii u kilku różnych dostawców, by umożliwić sobie dostęp do danych na wypadek awarii jednej z chmur. Warto jest również pamiętać, że mamy nawet możliwość wyboru różnych lokalizacji geograficznych, gdzie mogą być „nasze chmury". Szerokie wykorzystanie magazynów w chmurze jest trendem, za którym zdecydowanie będzie podążać wielu producentów systemów do backupu danych.

Praca zdalna zrodziła także potrzebę zapewnienia dostępu do systemu kopii i odtwarzania awaryjnego z dowolnego miejsca. Istotnym jest, by pracownicy zdalnie nie mieli z tym problemu w żadnej sytuacji, nawet gdy nie będzie działała lokalna infrastruktura, gdyż obecnie często administratorzy są nieobecni w siedzibach firm (bo pracują zdalnie :)). Wspomniana potrzeba sprawiła, że rozwiązania działające w chmurze znacząco zyskały na popularności. Niektórzy producenci zdecydowali się na dostosowanie swoich rozwiązań do wymagań systemów chmurowych i dostarczają je w modelu cloud-delivery. Xopero Cloud jest usługą, która od lat cieszy się popularnością i podążając za trendem nasze nowe rozwiązanie, Xopero ONE, będzie również dostępne w modelu cloud-delivery.

Lockdown i spowolnienie gospodarki na całym świecie to skutki pandemii, które również

mają swoje odzwierciedlenie na potrzebach użytkowników. Koszt oprogramowania zawsze jest jednym z istotnych kryteriów wyboru i nie dotyczy to jedynie systemów do backupu. Nie mówię, że jest to jedyne kryterium, ale kiedy porównujemy dwa rozwiązania o podobnych możliwościach, to znaczenie tego kryterium wzrasta. Mówiąc o koszcie, nie mam na myśli jedynie ceny zakupu rozwiązania, ale również koszt związany z jego obsługą, czy utrzymaniem niezbędnej infrastruktury. Taka sytuacja zdecydowanie sprzyja rozwojowi nowych rozwiązań, o nowoczesnej architekturze - które bez problemu mogą działać jako usługa w chmurze, nie wymagając od użytkownika utrzymywania dodatkowych maszyn - lub na obecnie posiadanej infrastrukturze, by nie generować dodatkowych kosztów. Nie bez znaczenia będzie tutaj również możliwość automatyzacji procesów, czy intuicyjność obsługi, by bez potrzeby szkoleń móc zminimalizować czas potrzebny na przygotowanie kopii czy, co istotniejsze, odtwarzania danych.

Z zadowoleniem mogę powiedzieć, że wśród użytkowników, przedsiębiorców, administratorów rośnie świadomość potrzeby systemu, który efektywnie zabezpieczy ich dane. Zdecydowanie częściej wiedzą, że dane, którymi operują na co dzień są istotne, że mogą je utracić, a kary nakładane przez UODO, o których możemy czytać, przypominają o odpowiedzialności za te dane. Natomiast jeśli mówić o zabezpieczaniu stacji roboczych, czy serwerów, to dominuje trend wykonywania kopii na poziomie obrazu dysku – staliśmy się użytkownikami danych, często nie wiedząc, gdzie właściwie się znajdują.

Zmiany, jakie zaszły na całym świecie w 2020 roku, znalazły swoje odzwierciedlenie w wyzwaniach stawianym producentom systemów do backupu i odtwarzania awaryjnego, którym muszą sprostać. Niektóre z rozwiązań są obecne na rynku od wielu lat w formie, która niewiele się zmieniła, a ich architektura jest już przestarzała. Producenci tych rozwiązań mają za sobą dług technologiczny, dodawanie nowych funkcjonalności trwa miesiącami, a czasem jest nieopłacalne lub nawet niemożliwe ze względu na wykorzystywaną technologię bądź architekturę samego systemu. Świat IT, gdzie w ułamkach sekund wykonywana jest niewyobrażalna liczba operacji, zmienia się bardzo dynamicznie, dlatego z pewnością warto obserwować nowości, jakie będą się pojawiać. Stay tuned!

Grzegorz Bąk
Product Development Manager, Xopero Software

Security Gaps
– czy to nadal problem, czy już katastrofa?

Organizacje na całym świecie borykają się z problemem braku wykwalifikowanych pracowników IT. Obecnie technologia rozwija się szybciej niż tradycyjna siła robocza. Według **Pew Research Center** zatrudnienie w zawodach STEM od 1990 roku wzrosło o 79% - z 9,7 miliona do 17,3 miliona.

Głównym wyzwaniem jest znalezienie i zatrzymanie doświadczonego personelu zajmującego się operacjami bezpieczeństwa oraz wystarczającej liczby analityków, aby odciążyć zespoły IT.

Kolejny problem dotyczy luk technologicznych. Zespoły SecOps używają średnio ponad 10 różnych kategorii narzędzi, w tym zapory ogniowe, zabezpieczenia poczty e-mail, zabezpieczenia punktów końcowych, analiza zagrożeń, czy do zarządzania lukami. W obecnej sytuacji są one jednak zwykle wyciszone, a ich implementacja słaba.

W tej sytuacji doskonalenie umiejętności zawodowych obecnych pracowników, zaczyna odgrywać kluczowe znaczenie w zapewnieniu odpowiedniej ochrony IT.

Z badania przeprowadzonego przez Cybrary dowiadujemy się, że 72 procent respondentów potwierdza, że w ich zespołach istnieją luki w umiejętnościach. Jeszcze bardziej niepokoi fakt, iż 65 procent menedżerów jest zdania, że braki w umiejętnościach mają negatywny wpływ na skuteczność ich zespołów. Luki w umiejętnościach wyraźnie zmniejszają wydajność i produktywność zespołów. Jednak 23 procent respondentów twierdzi, że ich organizacje nie stwarzają im możliwości dalszego rozwoju i podnoszenia kwalifikacji potrzebnych do odniesienia sukcesu w ich obecnej roli - a kolejne 30 procent wydaje się niepewnych.

Pomimo tego, specjaliści ds. IT i bezpieczeństwa pracują nad doskonaleniem swoich umiejętności we własnym zakresie, nawet jeśli jako istotne bariery zgłaszają koszty oraz brak czasu. Respondenci w zdecydowanej większości – ponad 62 procent - preferowali naukę online, w tym kursy, czy wirtualne laboratoria.

Według respondentów, specjaliści chcą podnosić swoje umiejętności zawodowe, przy czym 40 procent znajduje czas na naukę każdego dnia, a 38 procent przynajmniej raz w tygodniu. Prawie 48 procent poświęca na ten cel czas przed/po pracy. W weekendy swoje umiejętności doskonali co piąty ankietowany.

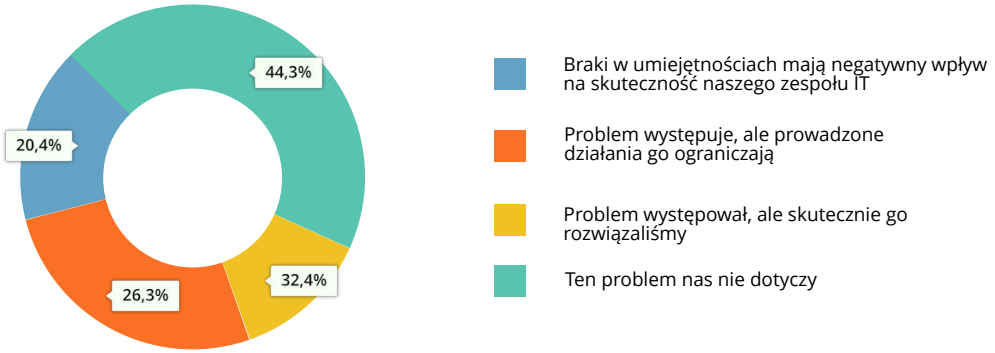
Wiele organizacji nie inwestuje w wystarczający sposób ani aktywnie nie wspiera rozwoju umiejętności swoich zespołów. Część respondentów uważa, że ich organizacje nie rozumieją, jakie umiejętności są wymagane od członków ich zespołu, a zaskakująca liczba organizacji w ogóle nie śledzi rozwoju umiejętności swoich specjalistów IT. Członkowie zespołów ds. bezpieczeństwa nie otrzymują pełnego wsparcia, jakiego potrzebują, aby poprawić umiejętności, ponieważ około 22 procent organizacji zmniejszyła budżet szkoleniowy, a 25 procent utrzymało je na tym samym poziomie co rok wcześniej. Jeszcze bardziej niepokojący jest fakt, że 16 procent respondentów twierdzi, że ich organizacje w ogóle nie dysponują budżetem szkoleniowym.

Czy z brakami w umiejętnościach mierzą się również

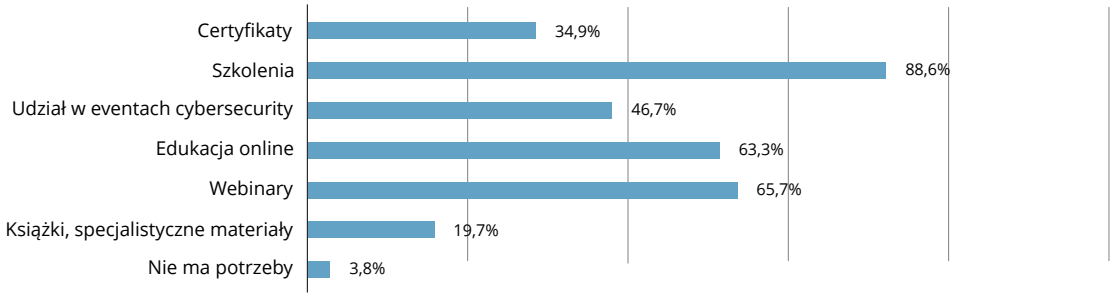
polscy specjaliści IT? Co prawda nikogo nie zaskoczy twierdząca odpowiedź na to pytanie, jednak sytuacja wydaje się być trochę lepsza niż na Zachodzie.
Z badania przeprowadzonego przez Xopero Software wynika, że ponad 55 procent ankietowanych w swojej codziennej pracy zetknęło się z problemem określanym mianem security gaps. W przypadku części z nich (20 procent) jest on na tyle poważny, że braki w umiejętnościach mają negatywny wpływ na skuteczność zespołu IT. Jednak 35 procent badanych stwierdziło, że problem albo został już zażegnany, albo prowadzone obecnie działania, skutecznie go ograniczają. Dodatkowo, 44 procent badanych jest zdania, że ten problem ich nie dotyczy.

W takim razie, jakie działania powinni podejmować pracodawcy, aby skutecznie zwiększać kompetencje zatrudnionych specjalistów IT? Ankietowani wskazali, że najistotniejsze z ich punktu widzenia są szkolenia (88 procent), webinaria (65 procent) oraz edukacja w modelu online (63 procent). Czy specjalistyczne certyfikaty, takie jak CEH, CompTIA czy też Security+, są chętnie pozyskiwane? I tak i nie. Z badania wynika, że specjaliści zdecydowaliby się raczej na udział w specjalistycznych eventach cybersecurity (46 procent). Jednak dostrzegają także wagę branżowych certyfikatów - część specjalistów skorzystałaby z możliwości ich zdobycia (34 procent).

W jakim stopniu Twoja organizacja doświadczyła problemu braku talentów tzw. security gaps?
Źródło: Xopero Software



Jakie działania powinna podjąć Twoja organizacja, aby podnieść kompetencje i umiejętności działu/zespołu IT?
Źródło: Xopero Software



Forrester Consulting w zeszłorocznej analizie **2020 State of Security Operations** wykazał, że zespoły ds. bezpieczeństwa nadal borykają się z rosnącym tempem, natężeniem i złożonością cyberataków. Badanie przeprowadzone na grupie ponad 300 specjalistów z całego świata ujawniło, że tylko 46 procent organizacji jest zadowolonych z możliwości jakie dają stosowane przez nich rozwiązania cybersecurity.

Od początku kryzysu COVID-19 liczba ataków niebezpiecznie wzrosła. Liczba skarg dotyczących cyberbezpieczeństwa składanych do działającego w ramach FBI Internet Crime Complaint Center (Centrum Skarg Dotyczących Przestępstw Internetowych) od początku pandemii wzrosła o 200-300%.

Według danych Forrester aż 79 procent przedsiębiorstw doświadczyło naruszenia bezpieczeństwa w ciągu ostatniego roku, z czego prawie 50 procent w ostatnich sześciu miesiącach. Dzieje się tak pomimo faktu, że większość organizacji ma wewnętrzne zespołu bezpieczeństwa (SOC) lub stosuje jakąś formę monitoringu zdarzeń (24×7).

Jak jesteśmy już przy kwestii monitoringu, przyjrzyjmy się problemowi natężenia powiadomień. Według zebranych danych zespoły otrzymują dziennie średnio ponad 11 000 alertów bezpieczeństwa. Raport wykazał również, że większość organizacji nie jest w stanie zająć się większością lub wszystkimi otrzymanymi alertami. Niepokojący jest również fakt, że 28 procent alertów nie jest w żaden sposób adresowanych.

Inwestycja w pracowników

W raporcie **International Information System Security Certification Consortium (ISC)²**, z listopada 2019 r. stwierdzono, że chociaż na całym świecie pracowało wówczas około 2,8 miliona specjalistów ds. bezpieczeństwa, potrzeba jeszcze 4 milionów przeszkolonych fachowców, aby zlikwidować lukę w umiejętnościach w zakresie cyberbezpieczeństwa. To wzrost o 145 procent. Jednak mówimy o sytuacji sprzed wybuchu pandemii COVID-19.

Zamiast szukać wykwalifikowanych pracowników na zewnątrz, firmy powinny wyszukiwać talenty wewnątrz własnej organizacji i to tu inwestować środki.

Weźmy pod uwagę umiejętności, które posiadają zatrudnieni pracownicy: dogłębna znajomość struktur zespołu, procesów wewnętrznych, produktów, klientów, tego, co dostarczasz klientom lub użytkownikom końcowym, a także doświadczenia użytkowników. Tego rodzaju wiedza instytucjonalna jest bardzo cenna. Tymczasem nowi pracownicy zdobędą ją dopiero po długim czasie. Natomiast nauka umiejętności technicznych - nowego języka programowania, nowych algorytmów, nowych narzędzi do przetwarzania danych - może zostać opanowana stosunkowo szybko.

Organizacjom brakuje planowania strategicznego, jeśli chodzi o obszar cyberbezpieczeństwa. W rezultacie przedsiębiorstwa, które potrzebują wysoko wykwalifikowanych i zmotywowanych pracowników, nie podejmują właściwych kroków w celu rozwoju tych talentów. Około 68 procent uczestników badania **Life and Times of Cybersecurity Professionals 2020** nie wierzy, że ma dobrze zdefiniowaną ścieżkę kariery. Około 52 procent ankietowanych uważa, że umiejętności praktyczne liczą się najbardziej, a 44 procent, że równie ważne jest doświadczenie praktyczne (połączone z certyfikatami).

Żadne pojedyncze działanie (finansowanie, programy studiów, przekwalifikowanie itp.) nie służy wypełnieniu luki w umiejętnościach w zakresie cyberbezpieczeństwa. Potrzebne jest holistyczne podejście do ciągłej edukacji w zakresie cyberbezpieczeństwa. Począwszy od edukacji publicznej, wszechstronny rozwój kariery, a także zapewnienie większej wiedzy na temat bezpieczeństwa pracownikom IT, programistom, architektom i analitykom danych itp.

Covid-19 a praca zdalna

Szybkie przejście z pracy stacjonarnej na pracę zdalną, wymusiło wprowadzenie szeregu zmian w zespołach

zajmujących się siecią i bezpieczeństwem. Działy IT musiały położyć większy nacisk na współpracę i narzędzia połączeń zdalnych, zapewniając jednocześnie ochronę swoich pracowników i firm. Przejście od sieci lokalnej (LAN) lub łączności biurowej do wirtualnej sieci prywatnej (VPN) lub środowisk zwirtualizowanych spowodowało samo w sobie niezliczone problemy. Chociaż firmy cieszą się pewną ochroną dzięki zewnętrznemu hostingowi niektórych usług publicznych, takich jak ich strony internetowe lub systemy poczty e-mail, muszą dokładnie rozważyć swoje sieci VPN, a także inne usługi, które nie są hostowane ani chronione zewnętrznie.

Sieci VPN są łatwym celem ataków. Fakt, że większość firm używa nazwy „VPN" jako części adresu URL lub nazwy hosta, również ułatwia atakującemu zidentyfikowanie serwera. Dzięki pojedynczemu wyszukiwaniu systemu nazw domen (DNS) atakujący ma adres IP i może przeprowadzić konwencjonalny wolumetryczny atak DDoS za pośrednictwem wynajętej sieci botów w celu zasypania obwodów lub użyć ataku opartego na protokole sieciowym w celu sparaliżowania zasobów systemowych.

Kryzys COVID-19 przyspieszył przejście na pracę zdalną o 5-10 lat. Wiele firm posiada pracowników wykonujących swoje zadania zdalnie lub takich, którzy dużo podróżują. Ogłoszenie pandemii w 2020 oraz przykaz wysyłania możliwie jak największej liczby pracowników na pracę zdalną, oznaczało wprowadzenie tego modelu pracy przez podmioty, które nigdy wcześniej nawet go nie rozpatrywały. Pracownik mobilny zawsze stanowił interesujący cel dla atakujących, jednak teraz mamy ich znacznie więcej.

Trend w kierunku pracy zdalnej był już w toku, gdy uderzył COVID-19. Pandemia przyspieszyła jednak te przejście do stopnia, którego nikt się nie spodziewał. Z tego powodu zespoły IT i bezpieczeństwa musiały w trudnych sytuacjach reagować na kryzys, a inauguracyjny indeks zagrożeń zwraca uwagę na wynikające z tego luki w cyberbezpieczeństwie i luki w zabezpieczeniach zgłaszane przez pracowników.

Amerykańska siła robocza jest obecnie zależna od domowych sieci Wi-Fi i niezabezpieczonych urządzeń roboczych, a bez niezawodnej łączności pracownicy mogą nie otrzymywać potrzebnej im ochrony. Narzędzia antywirusowe i wykrywające zagrożenia wymagają stałego połączenia sieciowego, aby skutecznie blokować ataki. Niehartowane laptopy lub inne urządzenia końcowe mogą również stanowić poważne zagrożenie dla bezpieczeństwa sieci przedsiębiorstwa. Badania przeprowadzone przez Morphisec i Ponemon Institute wykazały, że średni koszt udanego ataku na punkt końcowy wyniósł 8,9 mln USD w 2019 r.

Jak usprawnić pracę małego zespołu?

1. Inwestując w nowe rozwiązanie, upewnij się, że jesteś świadom wszystkich kwestii od któych zależy udane wdrożenie nowego rozwiązania. Niektóre parametry warte rozważenia:

- Czy otrzymujesz wszystkie potrzebne funkcje z góry, czy potrzebujesz zakupić dodatkowe komponenty lub nawet oddzielne produkty?
- Czy produkt jest skomplikowany do wdrożenia? Ile czasu zajmuje wdrożenie jednej instancji? 1000 instancji?
- Jakie są wymagania dotyczące konserwacji i aktualizacji? Jaka jest częstotliwość aktualizacji?
- Czy musisz stale weryfikować informacje z poziomu dashboardu użytkownika, czy może powiadomienia są dostarczane za pomocą SIEM?
- Jaki jest odsetek fałszywie pozytywnych powiadomień?
- Jakie rodzaje dane otrzymujesz i czy są one przydatne w analizie incydentów?

2. Nowe technologie wykorzystywane w rozwiązaniach security są zwykle innowacyjne. Jednak bardzo często mamy również do czynienia z produktami typu *point solution*. Zamiast inwestować w kilka wyizolowanych rozwiązań, sprawdź, czy istnieją producenci, którzy oferują wszystkie potrzebne Ci funkcjonalności w ramach jednej, skonsolidowanej platformy - EDR,

NGAV, UBA, network detection itp.

3. Praca specjalistów od bezpieczeństwa w dużej mierze jest zależna od otrzymywanych alertów. Jednak większość zespołów nie dysponuje ani zasobami, ani czasem aby weryfikować każdy z nich.

Polityka bezpieczeństwa powinna zostać tak zdefiniowana, żeby zespół zajmował się tylko powiadomieniami, które są istotne dla bezpieczeństwa organizacji. Mogą być to wyłącznie alerty oznaczone jako Krytyczny i Wysoki lub tylko Krytyczny. Inną metodą jest wybranie konkretnych lokalizacji - określone serwery - lub krytycznych danych. Upewnij się również, że monitorujesz alerty, które zostały automatycznie rozwiązane, ponieważ w niektórych sytuacjach może być one oznaką większej kampanii - alert może w tej sytuacji sygnalizować moment naruszenia sieci.

4. Nie chcesz niejako zostać sam z nowym produktem, który jest skomplikowany w obsłudze lub jeśli jego dokumentacja jest bardzo pobieżna. Dlatego zweryfikuj ze swoim dostawcą lub vendorem:

- Ile szkoleń z obsługi produktem otrzymasz? Czy poniesiesz dodatkowo koszt wdrożenia? Czy jest jakiś koszt wstępnej konfiguracji?
- Czy w przypadku wystąpienia incydentu masz do dyspozycji wsparcie telefoniczne?
- Co zawiera się w SLA?
- Jaki posiadasz poziom wsparcia i zakres usług? Jakie są ich koszty dodatkowo?
- Czy prowadzisz obsługę techniczną na wypadek incydentów (inaczej MDR)?
- Jakie masz poziomy i zakres usług serwisowych i jakie są ich koszty?
- Jak dostępny jest Twój zespół supportowy?

5. Coraz większa liczba vendorów oferuje rozwiązania SaaS, które skracają czas i koszty wdrażania a także późniejszego utrzymania. Najprawdopodobniej będą one dużo mniej kosztowne niż ich lokalne alternatywy. Ponadto wiele technologii cybersecurity jest bardziej efektywnych jeśli ich architektura jest oparta na chmurze – większe możliwości przetwarzania.

Należy jednak mieć na uwadze, że część rozwiązań SaaS będzie nadal wymagać agentów zainstalowanych na urządzeniach końcowych. Co nie zmienia faktu, że ten typ architektury umożliwia szybkie i łatwe wdrażanie technologii, zapewnia „lekkość" agentów, centralny serwer zarządzania – i co najważniejsze ostatecznie zmniejsza koszty bez narażania bezpieczeństwa Twojej organizacji.

Proactive Management (PM) odpowiedzią na braki IT?

Środowiska IT podlegają ciągłym zmianom. Weźmy pod uwagę choćby onboarding i offboarding użytkowników, aktualizacje i zmiany aplikacji, dodawanie nowych urządzeń itp. Wykorzystanie automatycznego skanowania sieciowego może zidentyfikować nowe urządzenia i dodać je do istniejącego już indeksu. Urządzenia off-boarded znikną z indeksowanej listy. Lista może również służyć jako kolejny punkt kontrolny aby upewnić się, że maszyna z której się nie korzysta, została usunięta. System pozwala również sprawnie czuwać nad stanem aktualizacji. A w sytuacji jeśli aktualizacja maszyny nie powiedzie się, zostanie wysłane automatyczne powiadomienie.

Na ile krytyczną kwestią są regularne szkolenia pracowników? Zakończony właśnie rok – jak i w zasadzie wcześniejsze lata - pokazał, że jest ona niesłychanie istotna. Większość naruszeń ma miejsce, gdy użytkownik nieświadomie umożliwia atakującym wtargnięcie do systemu. Chociaż rozwiązania Proactive Management nie odpowiadają bezpośrednio za szkolenie użytkowników, mogą znacznie usprawnić zarządzanie uprawnieniami itp. Gdy do sieci zostaną dodane nowe urządzenia, PM zidentyfikuje grupy użytkowników, którzy muszą przejść szkolenie wprowadzające. Rozwiązania antywirusowe i anty-malware zabezpieczają punkty końcowe, które mogą być narażone na zagrożenia. PM zawiera funkcje raportowania, które pokazują, w których miejscach

systemu doszło do wtargnięcia. W ten sposób możemy wyizolować grupę użytkowników, którzy mogą potrzebować więcej szkoleń aby sprawniej i świadomiej opierać się atakom.

Raportowanie i analiza danych mają kluczowe znaczenie, zwłaszcza jeśli chodzi o cyberbezpieczeństwo. Plany naprawcze można opracować, gdy organizacja wie, gdzie istnieją jej słabe punkty i luki. Bez tej wiedzy organizacje w najlepszym przypadku zgadują lub nie są w stanie podjąć żadnych kroków. Regularne raporty dotyczące stanu zabezpieczeń urządzeń i serwerów zapewniają kluczowe dane dla zespołów IT. Organizacje korzystające z PM są w stanie zweryfikować kiedy pojawiła się poprawka, które maszyny zakończyły już aktualizację, czy wystąpiły problemy, które maszyny miały problemy lub nadal wymagają aktualizacji. Gdy te informacje są dostępne, zespół IT może podjąć kolejne kroki w celu rozwiązania problemów i zidentyfikowania potencjalnych luk.

Tym bardziej, że zwykle będziemy mieć do czynienia z wektorami ataku bardzo różnego typu. Stąd konkluzja, że organizacje potrzebują warstwowego podejścia do cyberbezpieczeństwa. PM umożliwia zespołowi IT dokonywanie aktualizacji na szeroką skalę na wszystkich maszynach w sieci. Dodatkowo umożliwia szybkie wprowadzenie zmian na wszystkich urządzeniach końcowych. Raportowanie z PM ma również kluczowe znaczenie dla zrozumienia środowiska, czasu wprowadzenia poprawek i tego, co dzieje się na wszystkich typach endpointów. Zespół IT może skupić się na projektach, które zwiększają bezpieczeństwo całej organizacji, kiedy nie musi martwić się o łatanie harmonogramów lub poprawianie zabezpieczeń na pojedynczych maszynach.

Szyfrowanie dysków, jako środek bezpieczeństwa danych, w coraz większym stopniu wpływa na zespoły IT i ich listy priorytetów, ponieważ do środowisk organizacji dodaje się więcej urządzeń mobilnych i laptopów. Szyfrowanie to krytyczna procedura bezpieczeństwa, która chroni tajemnice handlowe i inne ważne dane biznesowe, ponieważ coraz więcej użytkowników przechodzi na komputery przenośne (laptopy) i podróżuje z nimi. PM nie tylko łata i szyfruje dane, ale może również zapewniać ochronę punktów końcowych za pomocą programów antywirusowych i przeciwdziałających złośliwemu oprogramowaniu.

Wczesne wykrywanie jest prawdopodobnie najważniejszą techniką zapobiegającą cyberzagrożeniom. Im ten czas jest dłuższy, tym szkód są w stanie wyrządzić atakujący. Średni czas wykrycia naruszenia przez organizacje to 6 miesięcy. Hakerzy dysponują więc wystarczającą ilością czasu na wyszukanie i wykradzenie wartościowych danych. Za sprawą rozwiązań PM zespół IT zyskuje więcej czasu na skupienie się na innych niezbędnych zmianach systemowych, które zapewniają bezpieczeństwo organizacji.

Jeśli dodamy do tego stack'a technologicznego narzędzia umożliwiające analizę behawioralną nowej generacji, heurystykę i uczenie maszynowe, jesteśmy w stanie wykryć zagrożenia i naruszenia stosunkowo wcześnie.

Technologia stała się nieodłączną częścią naszego codziennego życia, a jednym z jej kluczowych elementów - szeroko komentowanym i budzącym największe lęki - jest nasze bezpieczeństwo w jej użytkowaniu.

Codziennie słyszymy o naruszeniach bezpieczeństwa w małych jak i wielkich firmach. Co jakiś czas dowiadujemy się również o wyciekach danych z ambasad i organizacji rządowych krajów na całym świecie.

Przeciętny obywatel również nie wie, w jaki sposób chronić swoje dane i prywatność w sieci. Często nie jest również świadom utraty danych, bądź tego, że stał się ofiarą ataku.

Wniosek nasuwa się jeden – nikt nie jest w stu procentach bezpieczny, a w większości przypadków to my sami (ludzie) jesteśmy najsłabszym punktem każdego systemu cybersecurity.

Jak więc poradzić sobie z tym problemem?

Wielkie korporacje starają się minimalizować ryzyko naruszeń bezpieczeństwa inwestując ogromne pieniądze w cybersecurity własnej organizacji, by jak najlepiej chronić siebie i swoich klientów. Rozumieją, że inwestycja w sprzęt i oprogramowanie nie wystarczy, a kluczem do sukcesu jest maksymalnie profesjonalna kadra, której kształcenie nigdy się nie kończy.

Pozostali mają trudniej. Znaczna większość przedsiębiorstw, nawet jeśli chciałaby zatrudniać najlepszych, nie dysponuje jednak odpowiednimi argumentami by przyciągnąć takie osoby. Zatrudniają więc osoby o mniejszej wiedzy i doświadczeniu, w których plan rozwojowy trzeba włożyć niemałe sumy. Dodatkowo trzeba na to niestety poświęcić ogromne ilości czasu (często w czasie wolnym) by osiągnąć satysfakcjonujący poziom – koniec końców nawet to nie jest gwarancją sukcesu bezpieczeństwa organizacji.

Dziś każdy skuteczny manager IT, budując swój zespół, musi posiłkować się wiedzą z psychologii i Human Resources (lub mieć mocne wsparcie działu HR). W przeciwnym wypadku nie będzie mieć łatwego zadania, a oczekiwania są przecież wysokie, bowiem stawką jest bezpieczeństwo organizacji i jej klientów.

Technologia rozwija się szybciej niż jesteśmy w stanie edukować ludzi by sprostać zapotrzebowaniu i obawiam się, że w przyszłości ten trend będzie się tylko pogłębiać. Niemniej jednak, nie pozostaje nam nic innego jak robić co w naszej mocy by tę lukę wypełnić, jednocześnie dbając o wysoki standard bezpieczeństwa organizacji w których pracujemy.

Damian Jakrzewski
Quality&Operations Manager, Xopero Software

Co chwilę dowiadujemy się o skutecznie przeprowadzonych atakach, nawet na największe firmy zajmujące się cyberbezpieczeństwem! Pojawiają się doniesienia o nowych lukach Zero-day, a nawet Zero-hour. To skąd możemy mieć pewność, że zrobiliśmy wszystko co było możliwe w danej sytuacji?

Nie da się odpowiedzieć jednoznacznie na takie pytanie, ponieważ złożoność współczesnych środowisk teleinformatycznych i ilość zagrożeń, w tym także tych dla nas nieznanych (jak wspomniane luki zero-day), na to nie pozwala. Powinniśmy natomiast jak najlepiej szacować ryzyko i zarządzać nim. Można to zadanie delegować, ale wymaga to elastyczności we współpracy z Biznesem - określenia krytycznych informacji, danych, systemów, a następnie skalkulowanie ile kosztuje ich niedostępność lub utrata. A ponieważ raczej nikt nie może sobie pozwolić na akceptację ryzyka dużego wycieku danych czy sabotażu całego systemu IT, to istotnym elementem jest sprawdzanie poziom zabezpieczeń w firmie. Niestety bardzo dużo firm tego nie robi i nie są świadome ryzyka.

Przyjrzyjmy się zatem najpopularniejszym źródłom zagrożeń i poszukajmy rozwiązań.

Błędy sprzętowe i programowe (podatności)

Powinniśmy sprawdzać, czy nasze systemy nie są podatne na znane ataki. Przestępcy cenią sobie czas i chętniej uderzają tam, gdzie jest im łatwiej, np. wykorzystując luki w oprogramowaniu. Rozwiązanie jest proste - regularne skanowanie podatności od zewnątrz, jak i od wewnątrz organizacji. Po skanowaniu przychodzi czas na pentesty polegające na włamaniach w kontrolowany i bezpieczny sposób. Warto pamiętać, aby „badać organizację" regularnie. Nieustannie bowiem pojawiają się nowe podatności, zmieniają się systemy w firmie (aktualizacje, modyfikacje, rozbudowa).

Błędy ludzkie (błędy konfiguracyjne)

Zwrócę uwagę, że te błędy nie wynikają ze złej woli, tylko najczęściej z pośpiechu i braku odpowiedniej wiedzy. Firma jest tak dobrze zabezpieczona, jak dobry jest administrator systemów i świadomość użytkowników. Jedynym sposobem zapobiegania błędom są szkolenia pokazujące, jak można się włamać i jakich narzędzi używają cyberprzestępcy. Cykliczność szkoleń i stałe podnoszenie świadomości pozwalają zbudować odpowiedni poziom bezpieczeństwa w firmie. Istotnym aspektem jest także bieżące monitorowanie i przeglądanie logów, żeby odpowiednio wcześnie wykryć podejrzaną aktywność. Z pomocą SOC as a Service - doświadczonego zespołu ludzi można wesprzeć bieżący monitoring bezpieczeństwa oraz ulepszyć zabezpieczenia.

Brak szkoleń pracowników (Security Awareness)

Firma jest tak bezpieczna, jak jego najsłabiej wyszkolony pracownik. Niby truizm, ale ataki na różne organizacje pokazały że phishing oraz social engineering są potężnym i bardzo skutecznym narzędziem cyberprzestępców. Te niby banalne i znane od lat techniki „cieszą się" dużą skutecznością. Dlatego tak ważna jest ochrona skrzynek e-mail użytkowników oraz regularne szkolenia Security Awareness, najlepiej oparte na przykładach, czyli symulowanych kampaniach phishingowych. Dzięki profesjonalnym narzędziom możemy na podstawie wyników takich symulacji ocenić świadomość pracowników.

Braki dostępu do usług

W czasach pandemii i wszechobecnej pracy zdalnej wydaje się, że ochrona łącza firmy jest podstawą. Jednak od marca obserwujemy ponad pięciokrotny wzrost ataków DDoS. Atak nie musi być duży, ażeby firmę sparaliżować na cały dzień. Jak zatem ma poradzić sobie biznes, który opiera się wyłącznie na Internecie, jak np. e-commerce? Dotyka to także każdej innej branży, wystarczy sprawdzić czy działa poczta firmowa albo narzędzie do wideokonferencji. Za tym wszystkim stoją realne przychody, zatem taka ochrona w tych czasach to nie wygoda, ale konieczność.

Michał Kędzierski
Cloud & Cybersecurity Team Manager, Netia S.A.

Nowy porządek, niezmienne zagrożenia

Główne wektory zagrożeń IT pozostały niezmienne. Luki w wiedzy i świadomości użytkowników i w efekcie phishing, scam i wszelkiego rodzaju socjotechnika wiodą niesławny prym. W wyścigu zbrojeń, przestępcy są szybsi niż informacja i wiedza, która powinna być główną tarczą ochronną firm i ich pracowników. Rok 2020 zmienił jednocześnie całe otoczenie biznesowe, w którym żyjemy. Pandemia wywróciła stolik z kartami i ustanawia nowe porządki w organizacji pracy.

Ten rok był nie lada wyzwaniem dla większości przedsiębiorstw w aspekcie organizacji pracy i zapewnienia ciągłości działania. Prawdopodobnie 2021 zapewni nam równie wiele emocji. Niepewność, strach i dezinformacja osłabiają zdolności biznesu do budowania nowej „normalności". Z perspektywy działów IT oczywistym wyzwaniem 2020 roku było masowe przenoszenie organizacji na pracę zdalną. Firmy stanęły w obliczu konieczności przygotowania infrastruktury oraz dostosowania sprzętu i oprogramowania. Nikt nie był w pełni gotowy na tak nagłe zmiany. Tylko dzięki olbrzymiemu wysiłkowi świata IT, w tym zaangażowaniu dostawców, udało się zapewnić niemal natychmiastową reorganizację i powszechną dostępność niezbędnych narzędzi. Odejście od norm to jednak idealna okazja dla każdego rodzaju kryminalistów. Cyberprzestępcy również wykorzystali tę okazję, w tym zmiany w procedurach, zachowaniach użytkowników, czy nieznajomości nowych narzędzi. Liczba ataków rośnie znacząco. Szczególnie w marcu i kwietniu widać było eksplozję wiadomości phishingowych związanych z koronawirusem, ataki na komunikatory, dystrybucji fałszywych linków, próby przechwytywania tożsamości. Gdzieniegdzie jesteśmy przywiązani do wiekowych technologii. E-mail oraz stare protokoły tj. IMAP, SMPT, POP3 nie obsługują np. wieloskładnikowego uwierzytelniania i nie wytrzymują pod naporem agresywnych ataków.

Większość specjalistów IT uważa, że pracownicy zdalni stanowią większe niebezpieczeństwo dla firmy oraz traktują wprowadzenie trybu pracy jako zagrożenia dla bezpieczeństwa danych. W czasie pandemii zwiększyła się odpowiedzialność biznesowa działów IT. W przypadku awarii lub wycieku danych, to właśnie do nich władze firmy zwrócą się po wyjaśnienia. Logowanie się z prywatnych laptopów, ograniczenia w dostępie do sieci VPN, korzystanie z pozafirmowych sieci Wi-Fi oraz masowe użytkowanie aplikacji do wideokonferencji to tylko niektóre ze zmartwień administratorów sieci. Przenikanie życia prywatnego z służbowym powoduje ograniczenie czujności i naginanie wypracowanych procedur. Infekcje po stronie aktualizacji czy instalatorów różnego rodzaju software'u powinny uczulić na konieczność weryfikacji każdej nowej wersji i programu na służbowym sprzęcie. Zarządzanie całością zasobów przez kompetentny i dobrze wyposażony dział IT może minimalizować ryzyka.

Jak pokazały ostatnie miesiące, bezpieczeństwo IT nie jest wyłącznie sprawą pojedynczych organizacji. Firma czy instytucja publiczna staje się bezbronna wobec ataków, które daleko wykraczają poza standardowe ramy. Przestrzeń cyfrowa jest też areną rozgrywek grup przestępczych, służb specjalnych wielu krajów czy grup działających na zlecenie. Jesteśmy świadkami ataków, których ofiarami są klienci i użytkownicy software'u od globalnych vendorów. Powinniśmy uwrażliwić pracowników na konieczność stosowania „ograniczonego zaufania". Stosujmy procedury, które nawet w razie wycieku czy utraty danych zminimalizują straty. Ograniczanie dostępów do zasobów, minimalizacja przetwarzania danych, monitorowanie zdarzeń na urządzeniach końcowych, centralne zarządzanie sprzętem i oprogramowaniem, szyfrowana komunikacja to tylko niektóre punkty elementarza IT. W Axence rozwijamy te narzędzia z myślą o zarządzaniu IT w czasach pracy zdalnej. Analizujmy scenariusze ataków, edukujmy i informujmy użytkowników. Bądźmy lepiej przygotowani na 2021.

Grzegorz Oleksy
Prezes Zarządu, Axence

Cybersecurity gaps postrzegam w dwóch płaszczyznach. Z jednej strony jako brak odpowiednio wykwalifikowanych specjalistów, a z drugiej jako brak odpowiedniej edukacji wśród pracowników firm.

Na temat tego, jak lockdown przyspieszył digitalizację usług zostało już wiele powiedziane i należy to uznać za fakt. Powszechna cyfryzacja to oczywiście rosnąca ilość danych i procesów, które trzeba zabezpieczyć. Nietrudno się więc domyślić, że zapotrzebowanie na kompetencje związane z zapewnieniem bezpieczeństwa będzie rosnąć. Microsoft opublikował raport (źródło: **Official Microsoft Blog**), w którym szacuje, że do 2025 roku w Polsce powstaną 52 tysiące, a na świecie ponad 6,3 mln nowych miejsc pracy w obszarze cybersecurity.

Odpowiedzią na takie zapotrzebowanie w tym obszarze mogą być szkoły programowania, które dynamicznie dostosowują programy edukacyjne do biznesowych potrzeb rynku.

Masowa zmiana trybu pracy na zdalny oraz migracja usług i danych do chmury dodatkowo uwypukliły problem braku odpowiedniej edukacji związanej z ogólnym bezpieczeństwem wśród pracowników firm.

Niezabezpieczone laptopy, do których dostęp mają często członkowie rodziny czy odwiedzający ich goście, to tylko jedno z ryzyk. Warto więc zainwestować czas i wdrożyć w firmie choćby podstawową politykę bezpieczeństwa. To nie musi być wielostronicowy dokument, wystarczą podstawowe zasady spisane w punktach:

- stosuj dwuskładnikowe uwierzytelnienie wszędzie tam, gdzie jest to możliwe (poczta, dysk, systemy finansowe, social media, crm, itd.)
- używaj menadżera haseł (np. LastPass, czy Dashline), dzięki czemu hasła nie będą się powtarzać i będą trudne do złamania
- wykonuj regularnie backupy, dotyczy zarówno danych przypisanych do konkretnego konta, jak i danych współdzielonych w całej firmie
- regularnie aktualizuj oprogramowanie
- nigdy nie zostawiaj niezabezpieczonego komputera, zarówno w biurze, jak i w domu
- nie podłączaj do komputera przypadkowych i niezweryfikowanych pendrive'ów lub podobnych nośników danych
- nie nadawaj publicznego dostępu (o ile nie jest to bezwzględnie konieczne) do dokumentów na dysku firmowym (np. Google Drive), ponadto okresowo wykonuj

przegląd udostępnionych zasobów i ograniczaj niepotrzebne dostępy,

- w przypadku nieznanych nadawców:
  - sprawdź zgodność adresu e-mail z nazwą w polu from
  - nie otwieraj załączników (np. dołączone faktury)
  - weryfikuj linki przed kliknięciem

Oczywiście nie są to ani nowe, ani odkrywcze zasady, ale niestety wciąż mało powszechne. Ich stosowanie może bardzo skutecznie uchronić firmę przed stratami finansowymi czy wizerunkowymi.

Andrzej Kiesz

Współzałożyciel i prezes w infoShare Academy

Podsumowanie

2020 rok udowodnił, jak wiele aspektów naszego życia może być powierzonych komputerom, technologii i oprogramowaniu. Komunikatory umożliwiły nam pracę, kontakt z bliskimi, zastąpiły spotkania biznesowe, umożliwiały kontakty towarzyskie. Idąc dalej, zastąpiły przecież tradycyjne szkoły. Sklepy internetowe zdominowały zakupy, jeszcze większą popularność zyskały portale do zamawiania jedzenia online. Wymieniać można bardzo długo...

Technologie z jednej strony ułatwiły nam życie, a z drugiej, pokazały, jak łatwo nasze dane mogą zostać naruszone. W każdym z urządzeń, czy programów, z których korzystają firmy na całym świecie mogą zdarzyć się luki i błędy w zabezpieczeniach. Wystarczy, że trafią na nie przestępcy... A im chętniej wykorzystywana technologia, tym większe zainteresowanie nią hakerów. Wystarczy wspomnieć chociażby aplikację Zoom. Z uwagi na jej popularność, co tydzień informowaliśmy o nowych błędach lub atakach na ten znany komunikator.

Pamiętajmy, że po jednej stronie komputera zawsze siedzi człowiek - najsłabsze ogniwo systemu bezpieczeństwa IT. Nie bez przyczyny phishing od lat jest najczęściej wykorzystywanym wektorem ataku. Choć może wydawać się to niemożliwe, pracownicy nabierają się na maile z fałszywymi fakturami czy listami przewozowymi w załączniku i klikają w podejrzane linki. Jak się przed tym uchronić? Podstawą jest edukacja oraz zwiększanie świadomości zarówno o zagrożeniach jak i rozwiązaniach zabezpieczających na każdym szczeblu struktury organizacyjnej firmy. Działania te muszą być stałe - świat cyberbezpieczeństwa zmienia się jak w kalejdoskopie. A żeby za nim nadążyć, trzeba śledzić trendy, nowinki i innowacje. Dlatego już po raz trzeci opisujemy najpopularniejsze tematy, które kształtują branżę bezpieczeństwa IT.

Jeżeli w ciągu roku chcesz być na bieżąco z zagrożeniami (atakami, lukami i głośnymi wyciekami) oraz aktualizacjami i nowymi rozwiązaniami z zakresu bezpieczeństwa IT - **zapisz się na newsletter Centrum Bezpieczeństwa Xopero**. W każdy poniedziałek na skrzynkę mailową otrzymasz od nas przegląd najważniejszych i najgłośniejszych cyber-newsów minionego tygodnia.

W ramach uzupełnienia wiedzy polecamy również dodatkowe materiały edukacyjne, które prezentujemy w odrębnej sekcji tego dokumentu.

CYBERBEZPIECZEŃSTWO
bez tajemnic

Raport
Cyberbezpieczeństwo Trendy 2020

Pobierz dokument >

Raport
Cyberbezpieczeństwo Trendy 2019

Pobierz dokument >

Raport
Polski rynek cyberbezpieczeństwa

Pobierz dokument >

Kurs online
Data Protection Academy

Dołącz za darmo >

OFERTA
specjalna

Poznaj autorki raportu

Karolina Dzierżyńska

Centrum Bezpieczeństwa, Xopero Software

Pasjonatka nowych technologii. Od dziecka spoglądała w niebo i marzyła o odkrywaniu nowych planet. Dziś jednak nie skanuje przestrzeni kosmicznej - za to co poniedziałek przybliża wam newsy ze świata IT.

Szczególnie interesują ją tematy z obszaru robotyki, next-gen interface i uczenia maszynowego.
W tegorocznym raporcie spod jej pióra wyszły rozdziały poświęcone Internet of Things, Machine Learning oraz Security Gaps.

Marta Przybylska

Centrum Bezpieczeństwa, Xopero Software

Prawdopodobnie jedna z dwóch osób na świecie, której poniedziałek nie kojarzy się z porannym wstawaniem, a przygotowywaniem wysyłki Centrum Bezpieczeństwa Xopero.

Absolwentka dziennikarstwa i komunikacji społecznej, która swoje pasje do pisania i relacjonowania rzeczywistości realizuje obecnie w świecie nowych technologii. Uzależniona od informacji ze świata startupów, marketingu, podróży i przygód.

CENTRUM BEZPIECZEŃSTWA
XOPERO

Zapisz się

Autor raportu

Partnerzy