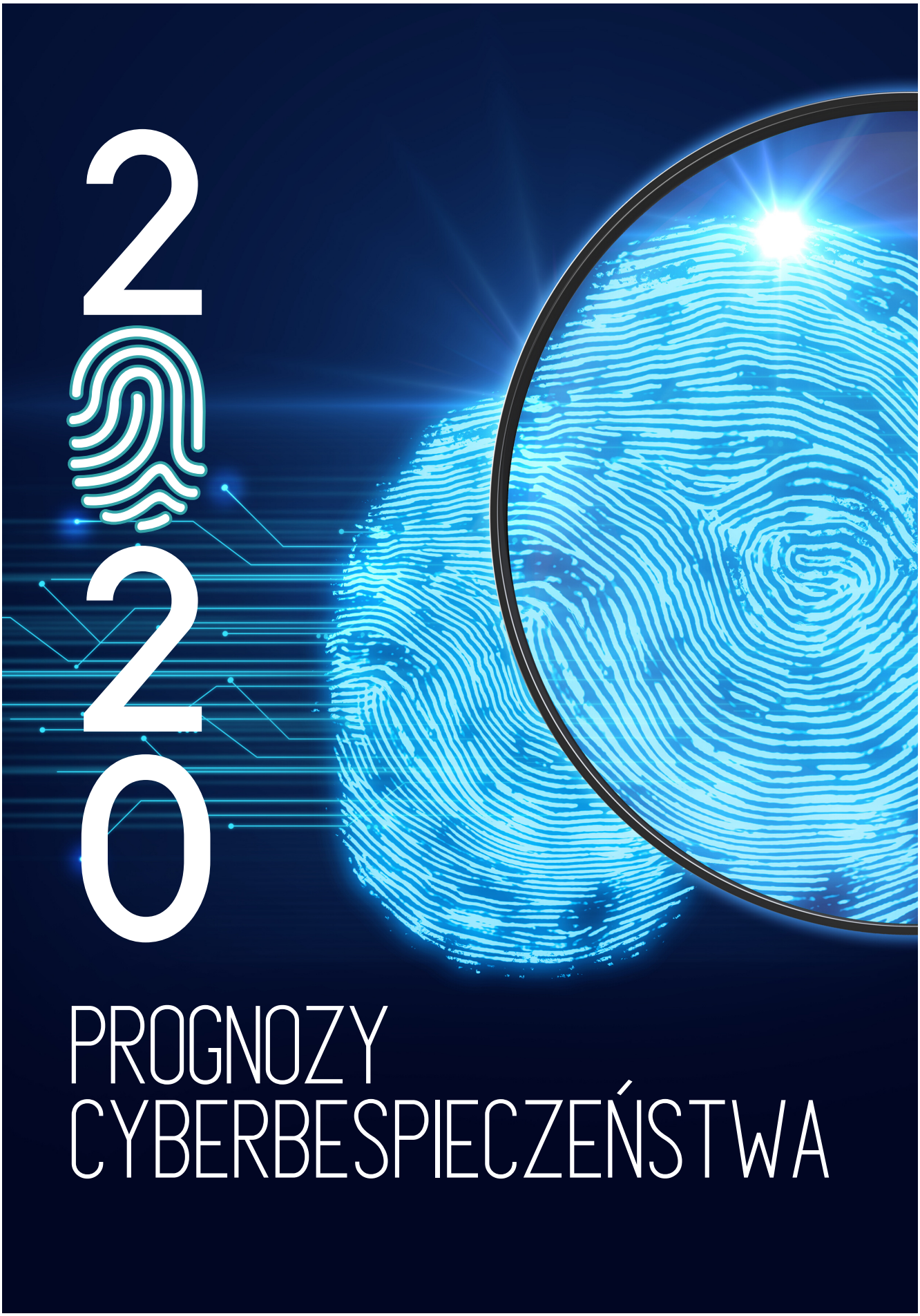
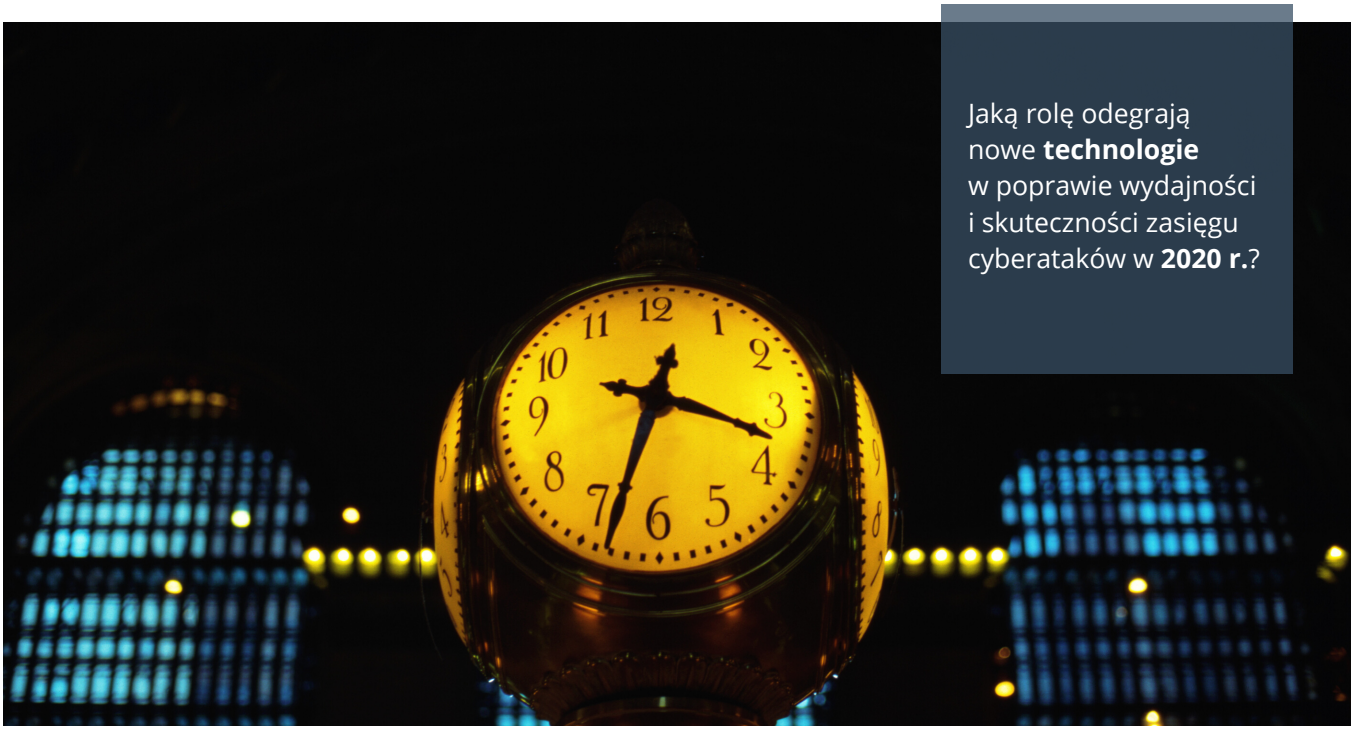


PROGNOZY CYBERBEZPIECZEŃSTWA

NET COMPLEX
Bezpieczeństwo IT

TYKAJĄCA BOMBA - RANSOMWARE. JAKI BYŁ 2019 ROK?

W miarę zbliżania się do końca roku, przyjrzymy się, które miejsce zajął 2019 na froncie cybernetycznym. Jakie były główne trendy obserwowane w ciągu ostatnich 12 miesięcy i jak możemy się przygotować na rok 2020 i kolejne lata?



Jaką rolę odegrają nowe **technologie** w poprawie wydajności i skuteczności zasięgu cyberataków w **2020 r.**?

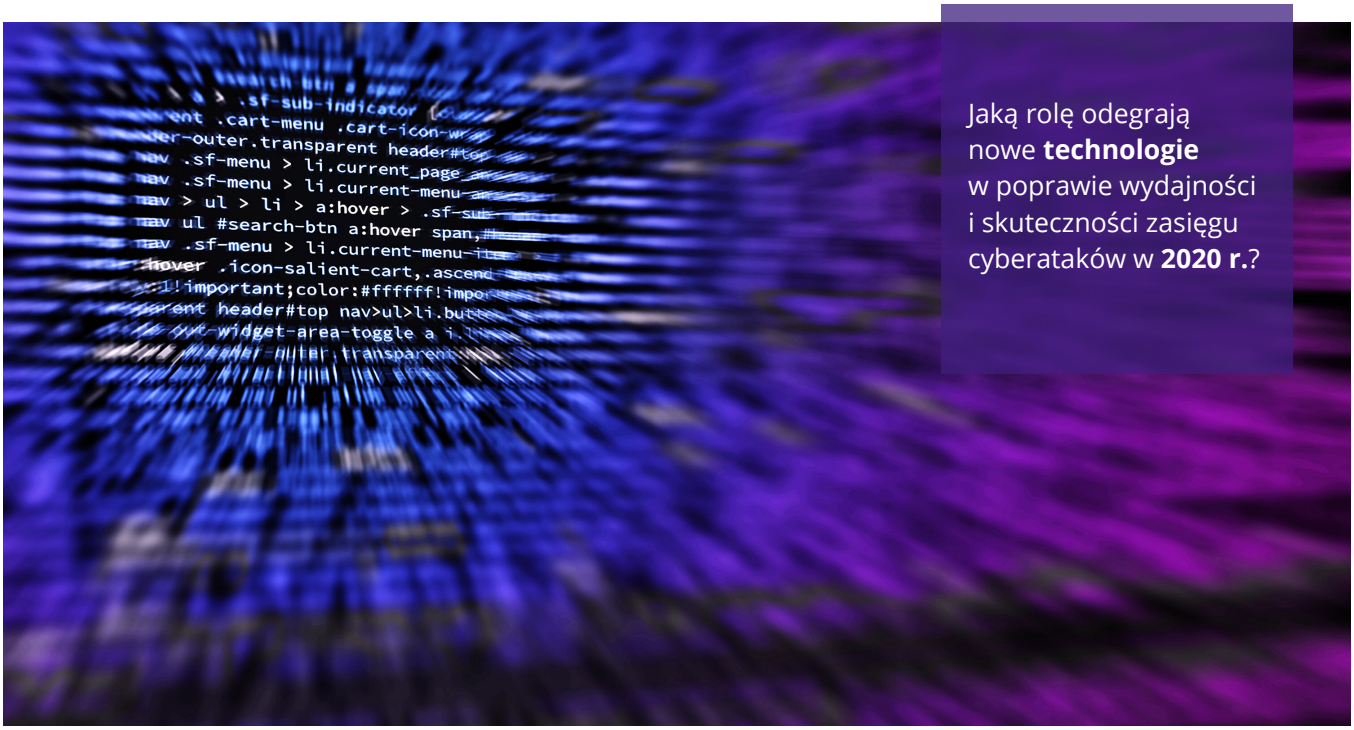
W 2019 roku mieliśmy do czynienia z bezprecedensową liczbą cyberataków na wszelkiego rodzaju organizacje, przy użyciu szerokiej gamy **zaawansowanych** technik. Najważniejszym spośród analizowanych cyberzagrożeń bez wątpienia stało się oprogramowanie ransomware, które dotarło do przedsiębiorstw na całym świecie. Ataki na łańcuch dostaw, omijające tradycyjne środki bezpieczeństwa cybernetycznego i włamujące się do systemów dostawców oraz oszustwa BEC, wykorzystujące połączenie phishingu i inżynierii społecznej do kradzieży dużych sum pieniędzy to tylko niewielka część góry lodowej cyberzagrożeń. W jaki sposób możemy chronić się przed atakami w 2020 roku oraz jakie będą najbardziej niebezpieczne zagrożenia w nadchodzących miesiącach? Aby odpowiedzieć na te i inne pytania, warto prześledzić, co na ten temat mają do powiedzenia eksperci z firm produkujących najpopularniejsze rozwiązania do ochrony sieci. Przeczytaj nasze prognozy i odkryj najlepsze wskazówki na nowy 2020 rok!

2019 rok był kumulacją ataków **ransomware**. Do najpopularniejszych według Centrum Bezpieczeństwa Internetowego (CIS) zagrożeń należały:

- Emotet
- Kovter
- ZeuS
- NanoCore
- Cerber
- Gh0st
- CoinMiner
- Trickbot
- WannaCry
- Xtrat

ZMNIEJSZA SIĘ BARIERA DOSTĘPU DO DANYCH

Zaskakujący i ciągły wzrost jest tym, czego możemy się spodziewać w **2020 roku.** Szokujące spotęgowanie ilości ataków hakerskich niestety dodatkowo podkreśli zwiększający się podział na „**mieć i nie mieć”** pod względem zwiększenia cybernetycznych polityk bezpieczeństwa i planowanych w związku z nimi inwestycji.



Jaką rolę odegrają nowe **technologie** w poprawie wydajności i skuteczności zasięgu cyberataków w **2020 r.**?

Chyba nikogo nie zdziwi już fakt, iż statystycznie **z roku na rok**, wskaźnik naruszeń bezpieczeństwa sieciowego diametralnie **wzrasta**. Wraz ze zwiększającą się liczbą cyberataków, równolegle wzmaga się ich różnorodność oraz zasięg oddziaływania. Bariera w dostępie do poufnych danych użytkowników ewidentnie się zawęża, co stanowi idealną przynętę dla cyberzłodziei. Zorganizowanie zaawansowanego ataku na przedsiębiorstwo i dobór do tego odpowiednich narzędzi nigdy nie było tak łatwe. Atak na sieć nie stanowi już większych trudności, nawet dla tych mniej doświadczonych hakerów. **Cyberprzestępcy stale rozwijają nowe techniki i metody ofensywy oraz eksfiltracji danych, przez co standardowe i podstawowe zabezpieczenia do ochrony sieci już po prostu nie wystarczają.**

Back to the future

Jak przewidują eksperci ds. bezpieczeństwa, największe zagrożenia w ciągu najbliższych kilku lat będą prawdopodobnie skutkiem stosowania przez administratorów nieodpowiednich i zbyt prostych praktyk w ochronie, a także występowania niezałatanych luk w zabezpieczeniach systemów informatycznych.

Ważne jest, aby nie patrzeć wstecz i skupić się na zagrożeniach, które czyhają w przyszłości. Firmy powinny w miarę szybko identyfikować pojawiające się ryzyko i zarządzać nim, posiadając program bezpieczeństwa obejmujący oprócz tradycyjnych sieci, **urządzenia IoT, OT oraz technologię przemysłu 4.0**. Bo jak przewidują prognozy, w 2020 roku, firmy będą musiały skupić się głównie na działaniach operacyjnych i produkcyjnych przedsiębiorstwa.

Według grupy IDG, **61%** organizacji doświadczyło incydentu związanego z bezpieczeństwem **IoT w 2019 r.** Globalna ekspansja Internetu Rzeczy i podłączonych urządzeń, korzystanie z chmury publicznej, PaaS i IaaS znacznie ułatwiają biznes i umożliwiają jego szybki rozwój. Jednoczesny i często niezauważany jest wzrost zewnętrznych ataków na organizacje.

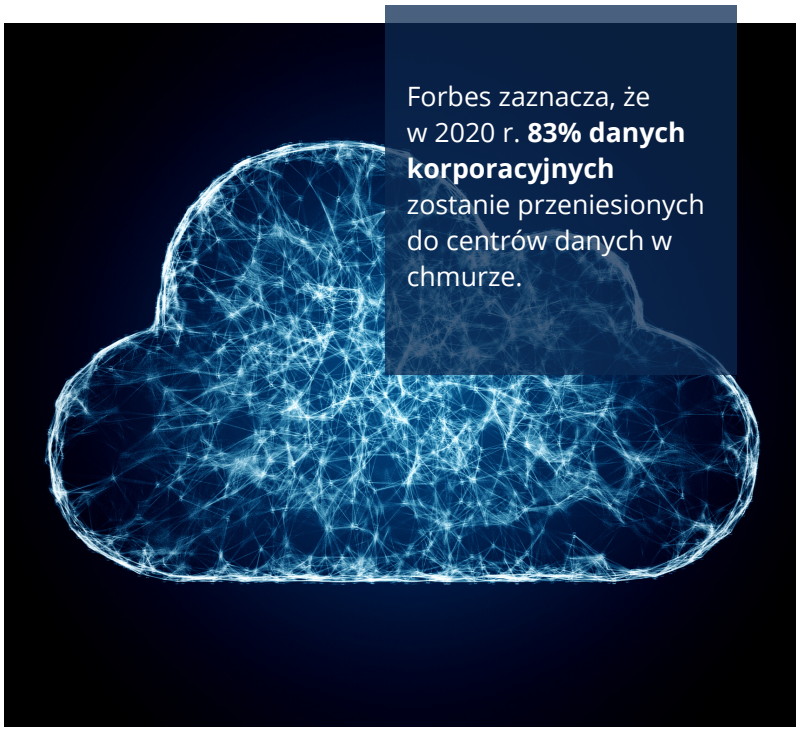
1 RANSOMWARE WKRACZA DO CHMURY

Preferowaną przez przedsiębiorców strategią jest multi-cloud **(84% przedsiębiorstw ją realizuje, z czego 58% korzysta z chmury hybrydowej).** Rośnie również zaadoptowanie chmury publicznej (91% wdrożeń) i wskaźnik inwestycji planowanych w tym obszarze (24% więcej niż w 2018 roku). Wyzwaniem nie jest już decyzja o **przeniesieniu** danych do chmury, ale raczej jej efektywne **zarządzanie i bezpieczeństwo.**

W ciągu ostatniej dekady, ransomware i jego różne odmiany zdawały się siać spustoszenie w firmach, niezależnie od branży. Podobnie, jak w poprzednich latach, eksperci IT przewidują, że oprogramowanie ransomware wcale nie odejdzie w zapomnienie, a wręcz przeciwnie - będzie ewoluować i skoncentruje się w większej mierze na **zasobach chmurowych**.

W 2020 roku, według badaczy z **WatchGuard Technologies**, atakujący mają preferować ukierunkowane ataki na branże, które nie mogą pozwolić sobie na jakiekolwiek przestoje. Należą do nich głównie, takie sektory, jak: opieka medyczna oraz usługi kluczowe (przemysł energetyczny, wodno-kanalizacyjny etc.).

Ponieważ organizacje każdej wielkości przenoszą zarówno swoje serwery, jak i dane do chmury, stała się ona kompleksowym centrum przechowywania wszystkich danych. W 2020 r. Eksperci spodziewają się, że „zasoby chmurowe" przestaną być bezpieczne za sprawą ataków ransomwar'a, który zacznie atakować chmurę, w tym magazyny plików, pakiety S3 oraz środowiska wirtualne.



Forbes zaznacza, że w 2020 r. **83% danych korporacyjnych** zostanie przeniesionych do centrów danych w chmurze.

W ciągu najbliższych kilku lat ryzyko ransomware w chmurze prawdopodobnie wzrośnie, jednak firmy wykorzystując nieodłączne zalety platform chmurowych, aktualizując kopie zapasowe i wdrażając najlepsze praktyki bezpieczeństwa, mogą skutecznie ochronić dane.

2 GDPR W STANACH ZJEDNOCZONYCH?

Po tym, jak dwa lata temu - **25 maja 2018 roku**, w europejskich krajach weszło w życie Ogólne Rozporządzenie o **Ochronie Danych Osobowych (RODO)**, wiele firm zdążyło już zostać ukaranych grzywnami w wysokości milinów euro za naruszenia przepisów **prywatności**. Jak dotąd niewiele miejsc poza UE jest regulowane przez podobne rozporządzenie. Niemniej eksperci są zgodni - w 2020 roku przepisy RODO będą również egzekwowane u naszych sąsiadów zza Oceanu.

W ostatnich latach, Stany Zjednoczone doświadczyły plagi **wycieków danych prywatnych**. W miarę rozwoju Internetu oraz aplikacji webowych, coraz więcej danych osobowych jest wykorzystywanych przez cyberprzestępców do różnorakich niecnych celów: m.in.: od ukierunkowanych manipulacji wyborczych, po nieetyczne wyłudzenia gotówki od ofiar. Obywatele USA zaczynają domagać się takiej samej ochrony prywatności, jaką cieszą się Europejczycy. Do tej pory tylko jeden stan - **Kalifornia**, odpowiedział na te żądania, uchwalając **Ustawę o Ochronie Prywatności Konsumentów (CCPA),** która - jak wiadomo - zacznie obowiązywać mieszkańców od początku 2020 roku.

Zachowaj ostrożność i wielką czujność podczas udostępniania **prywatnych** informacji w Internecie i sieciach społecznościowych. **Zapamiętaj:** W sieci nic nie ginie!

UKIERUNKOWANE ATAKI PODCZAS WYBORÓW 3

Eksperci wykazują, że wiele systemów z których korzystamy przy rejestracji wyborców i głosowaniu w dniu **wyborów**, posiada poważne **luki** w zabezpieczeniach cyfrowych.

Hackowanie wyborów w USA, stało się gorącym tematem już w 2016 r. W ciągu ostatnich czterech lat ataki obejmowały wszystko, zaczynając od dezinformacji rozpowszechnianej w mediach społecznościowych po rzekome naruszenia państwowych systemów wyborczych. Podczas wyborów prezydenckich w USA w 2020 r. przewiduje się, że zaatakowane zostaną stanowe i lokalne bazy danych, które wywołają niemałe zamieszanie w głosowaniu.

4 WZROST ATAKÓW PHISHINGOWYCH

24 lipca 2019 r. - **GreatHorn** opublikował raport, w którym eksperci ds. bezpieczeństwa odnotowali 25-procentowy **wzrost liczby wiadomości phishingowych**. Co najważniejsze - wszystkie zagrożenia, skutecznie ominęły podstawowe **zabezpieczenia sieci**, trafiając wprost do skrzynek odbiorczych użytkowników.

Badacze raportu **Email Security Trends, Challenges i Benchmark Survey** przeprowadzili ankietę wśród 1021 administratorów sieci z różnych branż, aby uzyskać wgląd w zagrożenia związane z pocztą e-mail i sposób, w jaki ci specjaliści bronią swoje systemy pocztowe.

Prawie połowa respondentów **(49,8 %)** odpowiedziała, że złośliwe wiadomości e-mail docierają do ich skrzynek odbiorczych co tydzień, pomimo stosowania wielowarstwowych strategii obrony. Te wyniki stanowią wzrost o **25 procent** w ciągu ostatniego roku. Respondenci stwierdzili również, że używają średnio więcej niż dwóch rozwiązań do bezpieczeństwa poczty e-mail.

Phishing jest popularny wśród hakerów. Zagrożenie w dalszym ciągu prosperuje bardzo dobrze, a ataki stają się coraz bardziej wyrafinowane i podstępne.

W 2020 roku, organizacje powinny wyjść poza tradycyjne narzędzia antywirusowe czy antyspamowe i wdrożyć urządzenia służące ciągłemu monitorowaniu sieci w celu wykrywania ataków phishingowych i zapobiegania im.

Raport **GreatHorn** pokazuje, że administratorzy odnotowują **25%** wzrost liczby wiadomości phishingowych **przechodzących** przez zabezpieczenia.

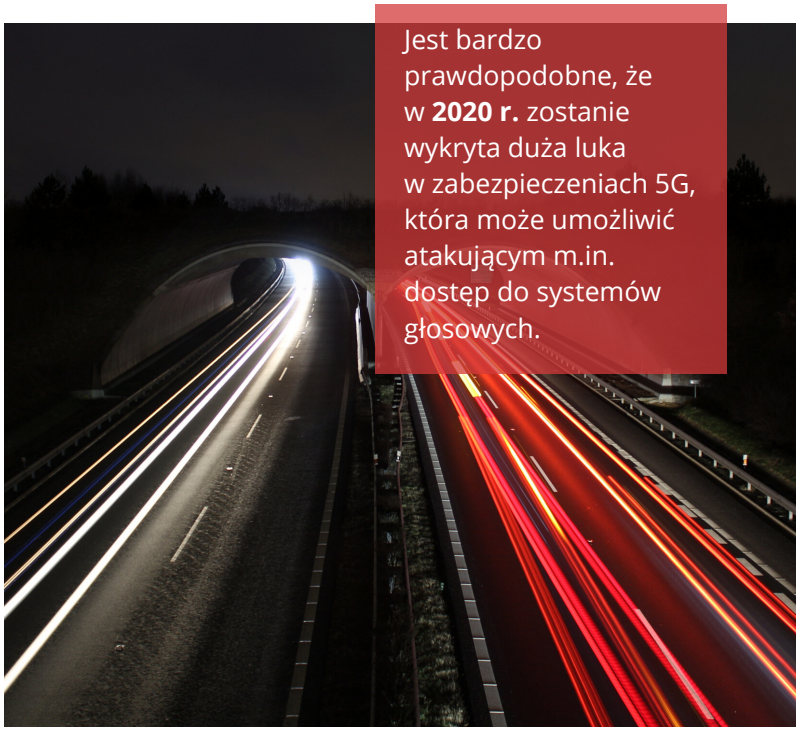
Microsoft przewiduje, że ataki phishingowe wzrosną w 2020 roku o około 260 % w porównaniu do roku 2019. Chociaż **phishing** za pośrednictwem połączeń głosowych („vishing") i wiadomości tekstowych („smishing") rośnie, e-mail pozostaje celem numer 1 w tego typu atakach. **Analitycy przestrzegają, że co najmniej jeden na 99 e-maili to atak phishingowy, z których wielu rozprzestrzenia oprogramowanie ransomware.**

5 POWAŻNE LUKI W ŁĄCZNOŚCI 5G

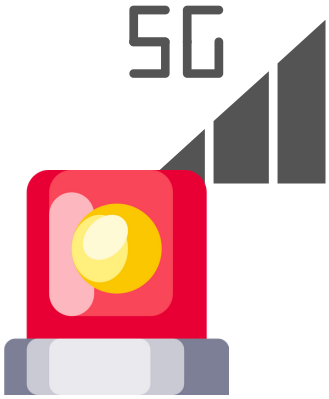
Jak przewidują prognozy, w 2020 roku **łączność 5G** spowoduje znaczny wzrost wykorzystania urządzeń IoT i przemysłowych systemów kontroli do ataków typu DDoS, phishingu, ransomware oraz kopania kryptowalut.

Pojawienie się i wdrożenie łączności 5G nie tylko zwiększa prędkość dostępu do sieci, ale co za tym idzie - stwarza idealne warunki do rozwoju nowego typu cyberzagrożeń. Integracja starszych sieci z 5G może w przyszłości skutkować, stworzeniem poważnych luk w zabezpieczeniach i w szyfrowaniu danych. Bezpieczeństwo sygnalizacji oparte na protokole IP może stać się nie do końca pewne i bardziej skomplikowane w monitorowaniu.

Wraz ze wzrostem świadomości ryzyka, firmy w 2020 roku, będą inwestować w narzędzia zapewniające prywatność i bezpieczeństwo, chroniąc tym samym dostęp do poufnych informacji.



Jest bardzo prawdopodobne, że w **2020 r.** zostanie wykryta duża luka w zabezpieczeniach 5G, która może umożliwić atakującym m.in. dostęp do systemów głosowych.



Rozwiązanie problemów z 5G wymagać będzie zasadniczych zmian w sposobie myślenia operatorów na temat sieci i bezpieczeństwa. Plan prewencyjny będzie musiał zostać dokładnie przemyślany - od urządzeń IoT, przez podstawową sieć korporacyjną, aż do oddziałów i wielu środowisk chmur publicznych.

6 DEFICYT SPECJALISTÓW

Według najnowszych badań prawie trzy miliony miejsc pracy związanych z bezpieczeństwem cybernetycznym pozostało niewypełnionych w 2018 r. Uniwersytety nie kształcą wykwalifikowanych kandydatów na tyle w szybkim tempie, aby zaspokoić zapotrzebowanie na nowych pracowników ds. bezpieczeństwa informacji. Trzy czwarte firm uważa, że w związku z deficytem umiejętności w zakresie cyberbezpieczeństwa, zmniejsza się również wskaźnik bezpieczeństwa sieci w firmach.

Deficyt specjalistów **IT Security** jest dobrze znanym problemem, który rośnie z roku na rok. Wykwalifikowanych kandydatów na to stanowisko staje się coraz mniej, a popyt rośnie. Według ISC2 do 2022 r. szacuje się, że 1,8 miliona miejsc pracy związanych z cyberbezpieczeństwem nie zostanie obsadzonych. Aby to pogłębić, amerykańskie Biuro Statystyki Pracy przewiduje, że liczba miejsc pracy w przestrzeni bezpieczeństwa wzrośnie tylko o 18 procent w okresie **2014-2024**.

Wniosek z tego jest prosty: W 2020 roku, powinniśmy poświęcić więcej czasu oraz budżetu na edukację społeczeństwa w zakresie szeroko pojętego bezpieczeństwa cybernetycznego.

SZTUCZNA INTELIGENCJA - MIECZ OBOSIECZNY 7

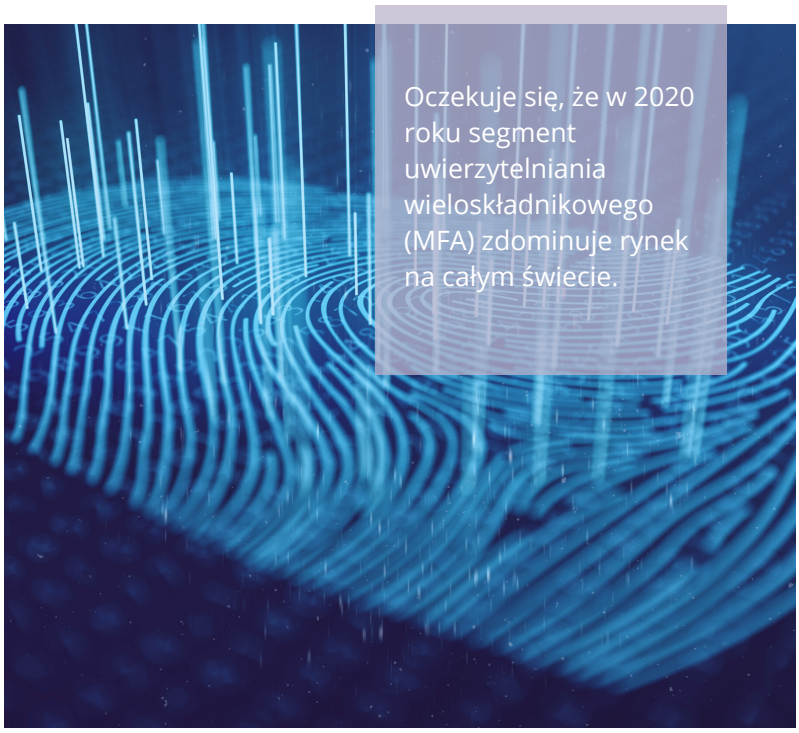
Jak wiadomo, sztuczna inteligencja i automatyzacja pomagają ograniczać ataki hakerskie. Prawdziwa moc AI pojawia się w połączeniu z głębokim **Machine Learning**, co wyjaśnia dlaczego stała się strategią wielu przełomowych technologii i rozwiązań oraz zarządzania usługami IT. Pomimo licznych plusów sztucznej inteligencji istnieje niestety również negatywna strona: zhakowanie systemów zasilanych AI prawdopodobnie doprowadzi do **ogromnych katastrof cybernetycznych**. Ataki na systemy cyberobrony, broń (fizyczną), wojny, samoloty mogą doprowadzić do niewyobrażalnych spustoszeń na całym świecie, osiągając kolosalny zasięg.
Jedno jest pewne: Sztuczna inteligencja to miecz obosieczny w tej cybernetycznej grze.

8 MFA STANDARDEM W ŚREDNIM BIZNESIE

Łatwość użycia MFA, zarówno w przypadku użytkownika końcowego, jak i administratora IT zarządzającego tymi narzędziami, wreszcie pozwoli organizacjom każdej wielkości rozpoznać korzyści bezpieczeństwa wynikające z dodatkowych czynników uwierzytelniających. Dlatego specjaliści przewidują, że *Multi-Factor Authentication* stanie się w 2020 roku standardową kontrolą bezpieczeństwa dla firm średniej wielkości.

Badacze z firmy **WatchGuard Technologies,** przewidują, że w 2020 roku uwierzytelnianie wieloskładnikowe (MFA) stanie się standardową kontrolą bezpieczeństwa dla firm z rynku średniej wielkości. Niezależnie od tego, czy będzie to spowodowane wyciekami miliardów e-maili i haseł do sieci, czy też licznymi zagrożeniami dla firmowych baz danych, nastąpi rozwój wieloskładnikowej autentykacji.

Pomimo licznych szkoleń dotyczących bezpieczeństwa w sieci, użytkownicy nadal tworzą zbyt proste do przejęcia hasła. To pokazuje tylko, że w dalszym ciągu nie jesteśmy w pełni świadomi zagrożeń, jakie czekają na nas w Internecie.



Wskazówka na **2020 rok** jest prosta - zaimplementuj MFA w całej organizacji. Wszystkie działania, zaczynając od codziennego logowania do komputera po dostęp do korporacyjnych zasobów chmurowych, powinny być powiązane z jakimś rodzajem uwierzytelniania **wieloskładnikowego.**

9 SYSTEMY BANKOWE NA CELOWNIKU

Specjaliści **Trend Micro przeczuwają**, że 2020 rok to wzrost **cyberzagrożeń w sektorze bankowym.** Banki będą na celowniku hakerów - chodzi głównie o oprogramowanie do bankowości internetowej oraz bankomatów. Operatorzy złośliwego oprogramowania mobilnego atakującego systemy bankowości internetowej i płatności będą bardzo kreatywni w 2020 r. jeśli chodzi o przejęcia haseł m.in. do internetowych kont bankowych.

Mobilne szkodliwe oprogramowanie atakujące bankowość internetową i systemy płatności będą jeszcze bardziej aktywne, z powodu zmiany w dyrektywie o usługach płatniczych Unii Europejskiej (UE) (PSD2).

Wdrożenie nowych zaleceń będzie miało negatywny wpływ na cyberbezpieczeństwo sektora bankowego - od wad interfejsów programowania aplikacji (API) po nowe ataki phishingowe.
Wzrośnie również nielegalna sprzedaż złośliwego oprogramowania. Na przykład warianty malware ATM, takich jak: Cutlet Maker, Hello World i WinPot, które można już bezproblemu dostać na czarnym rynku.

Banki powinny skupić się na współpracy z zewnętrznymi dostawcami usług IT dla wszystkich operacji bankowych. Powinny to być kluczowe plany na 2020 rok.

To na bankach spoczywa odpowiedzialność za ochronę danych swoich klientów przed cyberprzestępcami, a wyzwanie to będzie jeszcze trudniejsze w 2020 roku. Nie wiadomo, jakie zdarzenia zobaczymy w sektorze finansowym w przyszłym roku, ale jako przewidział główny oficer bezpieczeństwa informacji z Banku Rezerw Federalnych w Nowym Jorku: „Coś się wydarzy bez wątpienia".

10 ATAKI NA INTERNET RZECZY (IOT)

Urządzenia Internetu Rzeczy, pozwalają użytkownikom na zdalne kontrolowanie i zarządzanie zadaniami. W całym procesie generują i przesyłają wiele danych. Dane, które nie zostaną w bezpieczny sposób wymienione i przetworzone, mogą doprowadzić do naruszenia bezpieczeństwa cybernetycznego, a w konsekwencji do kradzieży, a nawet zniszczenia.

Badacze z F-Secure wydali zatrważające ostrzeżenie: cyberataki na urządzenia IoT przyspieszają w niespotykanym wcześniej tempie. W „Krajobrazie ataków na I półrocze 2019 r.", firma odnotowała trzykrotny wzrost ruchu związanego z atakami IoT. Firma korzysta na całym świecie z honeypotów - serwerów-wabików - podszywających się pod sprzęt operacyjny, aby przyciągać codzienne zagrożenia. W 2019 r. po raz pierwszy odnotowano tak wysoki wskaźnik ataków na te honeypoty. Naukowcy sprowadzili wzrost liczby ataków do wzrostu liczby urządzeń IoT wdrażanych na całym świecie. W ostatnich miesięcy mogliśmy zauważyć wiele ostrzeżeń dotyczących podatności takich urządzeń na atak. Wynika to częściowo z podstawowego braku ochrony w starzejącym się oprogramowaniu układowym lub architekturze. Często działy IT nie są nawet świadome wszystkich tych urządzeń w swoich sieciach, co sprawia, że łatanie problemów bezpieczeństwa jest prawie niemożliwe. „Od milionów do miliardów", tak eksperci z F-Secure w wielkim skrócie podsumowują swój raport.

W 2020 roku pojawią się nowe narzędzia umożliwiające ataki na IoT, ukierunkowane na coraz liczniejsze urządzenia konsumenckie.

Dobra rada na 2020 rok: Jeśli wiesz, gdzie i w jakiej ilości znajdują się wszystkie urządzenia **IoT**, zawsze staraj się je aktualizować i zabezpieczyć. To właśnie te urządzenia stają się najbardziej wrażliwym punktem dostępu do sieci domowych i biznesowych. Poza tym, prawie wszystkie ataki zaczynają się teraz od podjęcia działania przez człowieka - jego jednego kliknięcia i instalacji złośliwego oprogramowania - to prosta droga do przeprowadzenia ataku.

#JAK UNIKNĄĆ ZAGROŻEŃ?

W miarę zbliżania się końca 2019 r. przyjrzymy się, jak rok uplasował się na froncie cybernetycznym. Jakie były główne trendy obserwowane w ciągu ostatnich 12 miesięcy i czego możemy się z nich nauczyć, aby przygotować się na rok 2020 i kolejne lata?

Bądź czujny i proaktywny.

Najlepszą obroną przed takimi innowacyjnymi zagrożeniami jest po prostu praktykowanie dobrej cyberhigieny (tzn. unikanie klikania w podejrzane łącza lub załączniki od nieznanych użytkowników oraz posiadanie silnego systemu obrony : korzystanie z firewalli, systemów wykrywania włamań i zapobiegania. Odpowiednie szkolenia i sesje uświadamiające dla personelu i zespołów bezpieczeństwa mogą również pomóc w powstrzymaniu wszelkich prób włamań dokonanych przez złych aktorów. Posiadanie proaktywnego systemu analizy zagrożeń może pomóc Twojej organizacji wyprzedzić takie zagrożenia cyberbezpieczeństwa.

Rok 2019 to wyraźna kontynuacja poprzednich lat, jednak mimo wszystko **bardziej intensywna.** Więcej ataków, więcej naruszeń danych i większe szkody na całym świecie.

Co przyniesie 2020 rok? Czy zagrożenia będą się nasilać?

Myśl, która się nasuwa po 2019 roku jest następująca: Organizacje, większe korporacje, rządy i osoby prywatne muszą zacząć więcej inwestować w bezpieczeństwo informacji, edukację i zapobieganie cyberatakom.

Cyberprzestępczość to rozwiązywalny problem, - niekoniecznie musimy stać się jego ofiarą.

NET COMPLEX
Bezpieczeństwo IT

UL. WITA STWOSZA 5
43-300 BIELSKO-BIAŁA

TEL. 33 472 03 18
BIURO@NETCOMPLEX.PL