

PROGNOZY BEZPIECZEŃSTWA

NA ROK 2019

Prognozy cyberbezpieczeństwa stały się już tradycją. Po kolejnym minionym roku w zmieniającym się świecie cyberbezpieczeństwa, zagrożenia sieciowe niestety nadal ewoluują i to ze zdwojoną siłą. Każde prognozowanie niesie za sobą pewne ryzyko, szczególnie w branży IT.

Mgiełka „cyber-wojny” sprawia, że trudno dostrzec i ocenić każdy nowy trend pojawiający się na mapie zagrożeń. Niemniej jednak analiza i monitoring ryzykownych zachowań stały się istotną i solidną bronią w walce z cybernetycznym wrogiem.

Większość organizacji czyni z raportów kluczową część swoich programów bezpieczeństwa, by na ich podstawie przygotować organizacje niższego i wyższego szczebla na ostateczną walkę z cyberprzestępczością.

Próba przepowiadania zdarzeń i problemów w środowisku cybernetycznym - które w dużej mierze opierają się na nieobliczalnych ludzkich zachowaniach - jest bardzo trudna do wykonania.

Krajobraz zagrożeń jest ogromny, ofensywa i technologie obronne rozwijają się w zastraszającym tempie, a ataki hakerskie stają się coraz bardziej zaawansowane i powszechne.

Według tegorocznych raportów, w roku 2018, najgroźniejszymi zagrożeniami były:

- ataki phishingowe
- ataki zero-day
- ataki wewnętrzne
- zaawansowane ukierunkowane ataki typu DDoS
- złośliwe oprogramowanie, w tym wirusy, botnety, robaki, konie trojańskie



JAK DOKŁADNIE TO WYGLĄDAŁO?

Początek roku należał do ataków DDoS. W pierwszym kwartale 2018 zarejestrowano znaczny wzrost ataków botnetowych, w porównaniu z ostatnim kwartałem poprzedniego roku. Wzrosła nie tylko całkowita liczba ataków, ale też czas ich trwania – najdłuższy z ataków trwał blisko 297 godzin. Największy wygenerowany atak osiągnął wielkość 1,3 Tb/s. To dwa razy więcej, niż poprzedni rekord z 2016 roku. Nowe metody ataku korzystają z systemu Memcached, który pozwala zwielokrotnić dane użyte do ataku aż 500 tys. razy. Dzięki tej metodzie można przeprowadzać skuteczne ataki bez zaawansowanej wiedzy i kupowania specjalnych narzędzi na czarnym rynku, dlatego należy się spodziewać wzrostu wykorzystania Memcached. Jeden z pierwszych ataków botnetowych zarejestrowanych w minionym roku, stworzony został przez hakera amatora przy użyciu wiedzy dostępnej na forach hakerskich i wykorzystywał lukę zero-day w routerach Huawei. Atak został szybko powstrzymany, ale przestępcy nie udało się zidentyfikować.

Na pierwszym miejscu pod względem ilości przeprowadzonych ataków plasowały się niezmiennie Chiny (ponad połowa ataków). Przestępcy z zajmujących drugą pozycję Stanów Zjednoczonych, odpowiedzialni są jedynie za ok. 17% ataków.

W polskim internecie, największy ubiegłoroczny atak przeprowadzono na infrastrukturę DNS nazwa.pl. Atak podzielony był na dwa etapy, pierwszy trwający pół godziny, i drugi, trwający 2 godziny i 20 minut. W jego wyniku obciążenie serwerów nazwa.pl wzrosło dwudziestokrotnie w porównaniu z codziennymi godzinami szczytu. Powstrzymanie ataku umożliwiło wdrożenie technologii DNS Anycast, która umożliwia ładowanie stron www z najbliższego z rozproszonych na 6 kontynentach serwerów, co znacząco skraca czas reakcji na zapytanie.



Końcówka roku przyniosła doniesienia o pojawieniu się nowego wirusa. Goner rozprzestrzenia się za pośrednictwem popularnego klienta poczty email – Outlook. Plik dociera do użytkownika zakamufLOWany jako wygaszacz ekranu wraz z wiadomością: "How are you? When I saw this screen saver, I immediately thought about you I am in a hurry, I promise you will love it." (pisownia oryginalna). Uruchomiony plik, usuwa pliki programów antywirusowych zainstalowanych na komputerze i rozsyła się dalej, do wszystkich kontaktów zapisanych w programie pocztowym użytkownika.

Zwiększa się liczba raportowanych podatności w urządzeniach codziennego użytku podłączonych do sieci. Internet rzeczy oznacza coraz więcej urządzeń od różnych dostawców, które nie potrafią komunikować się ze sobą w sposób pozwalający na zneutralizowanie potencjalnych podatności. Wykryto już luki w elektronicznie sterowanych zamkach, które można otworzyć bez znajomości hasła, ale prawdziwego zagrożenia eksperci doszukują się w podatnościach jakie mogą skrywać inteligentne sprzęty medyczne jak np. rozruszniki serca.

Systematycznie wzrastała popularność koparek kryptowalut. Problem dotyka nawet największych serwisów www. Dla przykładu, pojawiły się doniesienia o obecności skryptów coin-hive w polskich serwisach należących do grupy Gazeta.pl. Kod trafia na stronę najczęściej za pomocą reklam zewnętrznych. Za granicą ofiarą koparek kryptowalutowych padli użytkownicy telewizji Showtime. Zagrożeni są także użytkownicy komputerów z systemem macOS, którzy decydują się na korzystanie z pirackiego oprogramowania Adobe. Malware OSX.DarthMiner udaje Adobe Zii, czyli nielegalne narzędzie pozwalające aktywować nieoryginalne kopie programów z rodziny Adobe.

Pojawiają się także wirusy, które podejmują decyzję o tym, czy zainfekowany komputer nadaje się do koparki kryptowalut, czy może potencjalnie bardziej opłacalne będzie zaszyfrowanie dysku za pomocą ransomware. Według raportu przygotowanego przez firmę Symantec,



WYCIEKI DANYCH W 2018 ROKU I OGROMNE STRATY

Najbardziej nośnym tematem, szeroko dyskutowanym w mediach, bo dotyczącym przeciętnych użytkowników, były wielkie wycieki danych przetwarzanych przez popularne aplikacje i przedsiębiorstwa. Chociaż wyciek danych użytkowników Facebooka na pewno należał do najgłośniejszych, nie był wcale najbardziej poważnym incydentem.

3 stycznia świat obiegła informacja o tym, że za cenę 500 rupii (26 złotych) reporterzy Tribune News Service nabyli za pośrednictwem WhatsApp dane logowania, pozwalające uzyskać dostęp do wszystkich numerów Aadhaar (odpowiednik polskiego numeru PESEL) zarejestrowanych w Indyjskim systemie ewidencji ludności. Tym samym reporterzy uzyskali dostęp do informacji, takich jak adresy e-mail, adresy zamieszkania, fotografie i numery telefonu. Za dodatkową dopłatą (300 rupii), uzyskać można było dostęp do oprogramowania pozwalającego wydrukować dokument tożsamości. W ten sposób wyciekły dane osobowe 1.1 miliarda obywateli Republiki Indii.

Na zachodzie, największy wyciek spowodowała wpadka amerykańskiego Exactis, przedsiębiorstwa zajmującego się marketingiem i gromadzeniem danych. Umieszczenie na publicznie dostępnym serwerze ponad 2 terabajtów danych, doprowadziło do ujawnienia danych osobowych 340 milionów amerykańców oraz przedsiębiorstw. To prawie czterokrotnie więcej niż w przypadku Facebooka



NA JAKIE CYBERZAGROŻENIA MUSIMY SIĘ PRZYGOTOWAĆ W 2019 ROKU?

Jak wynika z raportów, w dłuższej perspektywie, w 2019 roku i w przyszłości - powinniśmy się obawiać dwóch głównych technologii, które mogą wprowadzić niemałe spustoszenie w świecie cyberbezpieczeństwa. Są to techniki już istniejące i znane. Jedną z nich jest sztuczna inteligencja, która - jak przewidują prognozy - naprawdę zmieni krajobraz zagrożeń.

Drugie zagrożenie stanowi technologia kwantowa. Według badaczy, to właśnie do kwantów należy przyszłość. Dzięki tej metodzie, liczba zaawansowanych ataków diametralnie wzrośnie. Obliczenia kwantowe zmniejszą czas potrzebny na złamanie tradycyjnego szyfrowania nawet do kilku minut - gdzie w normalnych warunkach, potrwałoby to kilkanaście tygodni. Fizycy i matematycy są w trakcie ustalania algorytmów odpornych na kwantowanie, które skutecznie powstrzymają zagrożenia.

Najważniejszą innowacją w 2019 roku ma być również koncentracja na śledzeniu ruchu i widoczności sieci. Chodzi o monitorowanie procesu działania, aby obronić się przed atakami. Organizacje muszą zdawać sobie sprawę z tego co się dzieje - nie tylko skupiając się na aspektach stricte finansowych, ale na pobieranych plikach, maszynach wirtualnych, rozważając również wdrożenie uwierzytelnienia wieloskładnikowego, bowiem jak przewidują prognozy - w 2019 roku, te jednoczynnikowe autoryzacje nie wystarczą.



O TYLE WZROSNIĘ PRZECIĘTNA WARTOŚĆ OKUPU RANSOMWARE

Coraz częściej ofiarą ukierunkowanych ataków padać będą elementy infrastruktury publicznej. Dlatego należy spodziewać się wzrostu średniej wysokości okupu do nawet 20 tys. dolarów.

FALA RANSOMWARE ZAWĘŻY SIĘ, ALE NADAL BĘDZIE SIĄĆ SPUSTOSZENIE

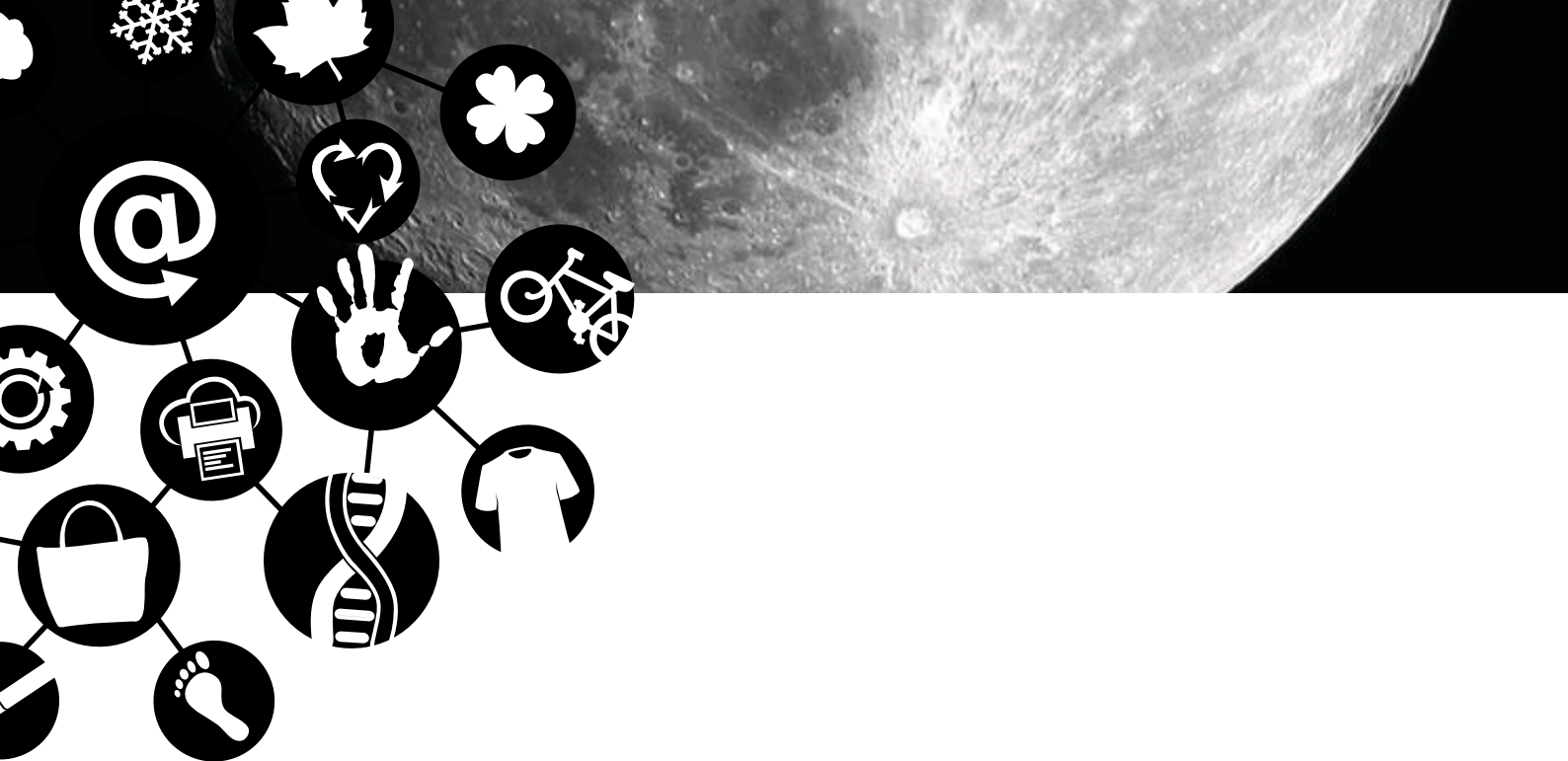
Ransomware, koparki kryptowalut, trojany bankowe i filtry VPN - to tylko niektóre z najgroźniejszych rodzajów złośliwego oprogramowania, które nadal zagrażają i będą zagrażać organizacjom w 2019 roku. Badania Malwarebytes'a i Kaspersky'ego ukazały, że rokowania tych zagrożeń zmieniały się czasie, ale końcowy wynik nie wypadł za dobrze. Eksperti są zgodni: Rok 2019 będzie zalewał nową falą ransomware.

Zwiększone niebezpieczeństwo będzie widoczne w takich rodzajach zagrożeń, jak ransomware, wraz z nową i ulepszoną jego odsłoną. Jedno jest pewne: Tradycyjny AV nie zapewni wystarczającej ochrony sieci.

Cybersecurity Ventures, przewiduje że koszty zniszczenia przez oprogramowanie ransomware przekroczy w 2019 roku - 11,5 miliarda dolarów.

W 2019 roku, kampanie ukierunkowane na ransomware będą koncentrować się na narzędziach i przemysłowych systemach kontroli (ICS). Średnie zapotrzebowanie za płatność wzrośnie o 6500 procent, co daje średnio od 300 do 20 000 USD za jednorazowy okup. Ataki te, będą skutkować realnymi konsekwencjami, takimi jak utrata dostępu do sieci oraz ważnych danych.

Ransomware nęka Internet przez ostatnie pięć lat, poczynając od CryptoLocker, kończąc na WannaCry, pierwszym szybko rozprzestrzeniającym się robaku. W ciągu ostatnich lat cyberprzestępcy przeprowadzali szeroko zakrojone kampanie ransomware, chcąc zarażać jak najwięcej ofiar, jednocześnie prosząc każdego o stosunkowo skromny okup - co prawdopodobnie ulegnie zmianie w 2019 roku.



IIOT - ROZSZERZENIE GRANIC POD KAŻDYM WZGLĘDEM

Nie musimy przypominać, że Internet Rzeczy rozwija się w błyskawicznym tempie. Pojazdy, sprzęt AGD, gadzety do noszenia, czujniki oraz oprogramowanie RFID połączone do sieci, to tylko niektóre z urządzeń, które w 2019 roku mogą paść ofiarą hakerów IIOT. Proces technologiczny cały czas brnie do przodu, powodując rozszerzenie sieci, a co za tym idzie - poszerzenie pola manewru cyberprzestępców.

Kierując się wygodą i korzyściami, jakie oferuje nam **IIOT**, musimy pamiętać o potencjalnych zagrożeniach i konsekwencjach ich wdrażania. Wiele organizacji sądzi, że ryzyko ataków na Internet Rzeczy jest minimalne. W 2019 roku w znaczący sposób, IIOT zademonstruje swój trend wzrostowy, zarówno w obszarze działalności, jak i w świecie cyberprzestępczym.

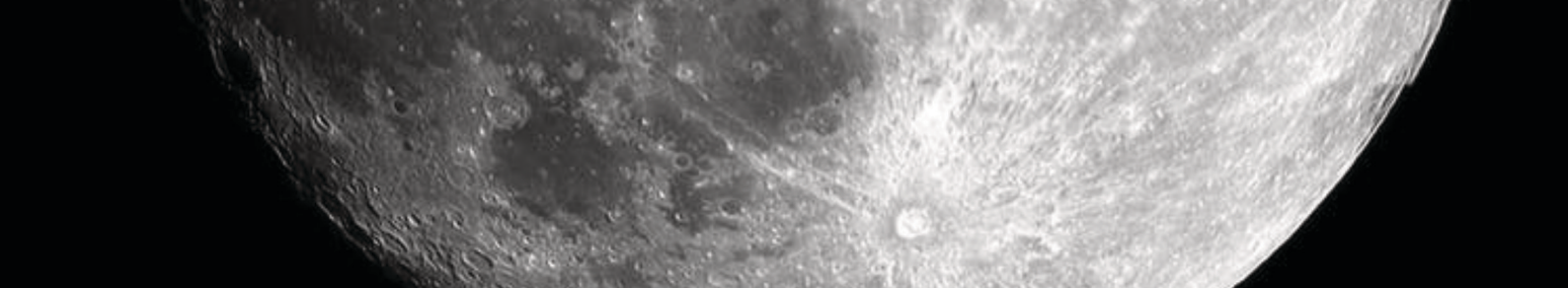
Prognozy na rok 2019 dotycząc IIOT są proste i zatrważające. Urządzenia IIOT narażone będą na ataki hakerskie i problemy z bezpieczeństwem.

Producenci sprzętu, tacy jak Cisco, HP, Dell i inni, budują specyficzną infrastrukturę, która ma być bardziej odporna fizycznie na zagrożenia. Zaopatrzenie się w rozwiązania chroniące punkty końcowe daje wgląd w stan sieci oraz obejmuje uprzywilejowaną kontrolę użytkownika i stosowanie tzw. białej listy aplikacji i programów.



ZDANIEM ACCENTURE, DO 2030 ROKU, GLOBALNY UDZIAŁ PRZEMYSŁU IIOT WZROŚNIE DO 14.2 TRYLIONÓW DOLARÓW. MORGAN STANLEY, SZACUJE Z KOLEI WZROST Z 90 DO 110 MLD DOLARÓW PRZED KOŃCEM 2020.

TYM SAMYM BLISKO DO 2020 , W UŻYCIU ZNAJDZIE SIĘ BLISKO 13 MLD URZĄDZEŃ I CZUJNIKÓW IIOT



ROK 2019 - ROKIEM CHATBOTÓW?

Bezpieczeństwo poczty elektronicznej nadal będzie dominować w krajobrazie zagrożeń, niemniej jednak, komunikacja online rozszerzy się poza wiadomości e-mail. Coraz częściej - według ekspertów z firmy **WatchGuard** - będą się zdarzać ataki ukierunkowane na konkretne osoby. Napastnicy zaprojektują chatboty, które będą przeprowadzać wstępną rozmowę z ofiarą, aby utworzyć przekonujący pretekst do ostatecznego wysłania jej linku phishingowego lub uzyskania danych osobowych. Atakujący będą badać szeroki zakres możliwości, w tym manipulowanie zamówieniami, instalację trojana zdalnego dostępu (RAT) na komputerze ofiary, a nawet wymuszenie.

Krótko mówiąc, w przyszłym roku atakujący zaczną eksperymentować ze złośliwymi chatbotami i technikami socjotechnicznymi. Wszystko zacznie się od podstawowych, prostych botów tekstowych, aby w przyszłości skupić się na bardziej zaawansowanych rozwiązaniach, wykorzystujących połączenia głosowe, rozmowy telefoniczne, takie jak np. Google Duplex - roboty imitujące człowieka.

GDPR - BÓL DOPIERO PRZED NAMI?

2018 był rokiem RODO. Nowe regulacje odnośnie przetwarzania danych osobowych, spędzały sen z powiek większości decydentów we wszystkich możliwych działach. W większości przypadków administratorzy stanęli przed wyzwaniem aktualizowania starych zgód dotyczących przetwarzania danych oraz wywiązania się z obowiązku informacyjnego, o którym mowa w rozporządzeniu.

Chociaż do tej pory do UODO wpłynęło ponad 600 skarg, nie nałożono jeszcze żadnej kary. Nie przeprowadzono też jak na razie żadnych większych kontroli. Dotychczas urząd skupiał się na interpretowaniu i wyjaśnianiu przepisów, w tym na udzielaniu odpowiedzi na ponad 70 zapytań, jakie wpłynęły do urzędu. Według raportu Deloitte, do najtrudniejszych zadań należy określenie roli stron w procesie przetwarzania danych osobowych. Wiele wątpliwości wzbudzają też postanowienia dotyczące profilowania danych, oraz zasady określania podstawy prawnej do ich przetwarzania. Warto pamiętać, że dla wszystkich, którzy mają wątpliwości co do tego jak w praktyce przystosować firmową politykę bezpieczeństwa, MSWiA opracowało specjalny kurs e-learningowy: „Zmiany w zakresie ochrony danych osobowych w związku z wejściem w życie RODO”

Według przewidywań, w 2019 roku będziemy oczekiwać pierwszej, olbrzymiej kary GDPR ukazującej dosadnie, że RODO to nie żart.

Kiedy ten dzień nadejdzie, organizacje nagle zaczną poważnie przyglądać się temu, co naprawdę muszą zrobić. Facebook, British Airways, Cathay Pacific itp. to tylko niektóre z wielkich korporacji, które poważnie ucierpiały w 2018 roku z powodu wycieku danych klientów.

CIEMNA STRONA MEDIÓW SPOŁECZNOŚCIOWYCH

W 2017 i 2018 roku media społecznościowe służyły jako platforma dla operacji informacyjnych i dezinformacji, kierowanych przez jednostki, partie polityczne i inne narody. Podczas gdy wiele dyskusji i przesłuchań trwało w Kongresie Stanów Zjednoczonych, UE oraz Wielkiej Brytanii, tak na prawdę niewiele osiągnięto.

W drugiej połowie 2018 r. **FireEye** ogłosiło rozległą sieć operacji informacyjnych - prawdopodobnie napędzanych interesem politycznym Iranu - obejmujących media społecznościowe. Wraz z nadchodzącymi wyborami w regionie Europy i Bliskiego Wschodu w 2019 roku, przewiduje się, że media społecznościowe będą nadal wiodącym narzędziem operacji informacyjnych, prowadzonych przez zagraniczne kraje. Tego typu kampanie będą trudniejsze do wykrycia ze względu na ich charakter. Wykrywanie i powstrzymanie ataku może okazać się wyzwaniem dla firm, działów informatycznych czy samego rządu.

W poprzednich prognozach mówiliśmy o rosnącym braku zasobów zapewniających bezpieczeństwo. Firmy nadal planują zatrudniać specjalistów ds. bezpieczeństwa, często zwracając się z prośbą o pomoc do firm zewnętrznych.

Outsourcing i współpraca z zewnętrznymi dostawcami usług zarządzanych, może pomóc firmom w rozwijaniu ich zdolności w zakresie cyberobrony.



KONIEC Z JEDNOCZYNNIKOWĄ AUTORYZACJĄ? BIOMETRYCZNE LOGOWANIE - ŁAKOMY KĄSEK DLA HAKERÓW

Biometryczne metody logowania, takie jak czytniki linii papilarnych na urządzeniach konsumenckich, typu: smartfon, tablet czy konsole do gier, będą stanowić w 2019 roku łakomy kąsek dla cyberprzestępców. Podczas gdy dane biometryczne są wygodniejsze i bezpieczniejsze niż skomplikowane hasła - są nadal niestety tylko jedną z metod uwierzytelniania. Jeżeli nie skupimy się na dodaniu drugiej formy autoryzacji, cyberprzestępcy, którzy z powodzeniem zhakują dane biometryczne, będą mogli łatwo i szybko uzyskać dostęp do cennych zasobów osobowych i finansowych firm.

16.8 MLD

WARTOŚĆ RYNKU
BIOMETRYCZNEJ
AUTENTYKACJI

(2017)

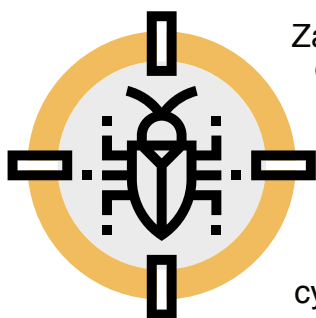
Czy, aby na pewno biometria jest łatwiejsza do złamania? W 2017 roku wietnamska grupa ds. bezpieczeństwa poinformowała, że stworzyła maskę, która może oszukać FaceID Apple. Znane są również inne przykłady ataków na biometryczne logowanie. To tylko kwestia czasu, zanim hakerzy udoskonalą te metody i wykorzystają rosnący trend biometrii jako jedynej formy uwierzytelniania.

Oczywiście, aby zapobiec tego typu atakom, najlepszym rozwiązaniem jest korzystanie z uwierzytelnienia wieloskładnikowego.

BEZPLIKOWY, „SAMOPRZYLEPNY” MALWARE „VAPORWORMS” WKRACZA DO GRY

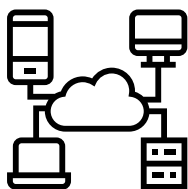
Ekspertci alarmują - w 2019 r. pojawi się nowy rodzaj szkodliwego oprogramowania, z właściwościami robaka, które pozwolą mu się rozprzestrzenić za pośrednictwem luk systemowych.

Bezplikowe złośliwe oprogramowanie jest trudniejsze do wykrycia tradycyjnymi rozwiązaniami zabezpieczającymi punkty końcowe, ponieważ działa całkowicie w pamięci, bez konieczności instalowania zainfekowanego pliku do systemu.



Zaawansowani atakujący wolą tę metodę, ponieważ bez szkodliwego pliku do skanowania, tradycyjne kontrole antywirusowe punktów końcowych mają problemy z wykrywaniem i blokowaniem zagrożeń bezplikowych.

W ubiegłym roku grupa hakerów znana jako Shadow Brokers spowodowała znaczne szkody poprzez wykrycie kilku luk w oprogramowaniu Microsoft Windows. Zaatakowanie systemu zajęło tylko miesiąc, doprowadzając do dwóch najbardziej szkodliwych cyberataków do tej pory - mowa o WannaCry i NotPetya.



CZY MASZ PEŁNY WGLĄD W CHMURĘ, W KTÓREJ PRZECHOWUJESZ DANE?

Czy widzisz, co dzieje się w chmurze, w której znajdują się Twoje dane? I czy jesteś w stanie skonfigurować centrum bezpieczeństwa (SOC), aby móc reagować na incydenty?

W 2018 roku pojawiło się wiele wyzwań związanych z chmurą. Spodziewamy się, że nastąpi kontynuacja oraz, że zagrożenia będą ewoluować. Dlaczego? Po pierwsze, wiele danych przenoszonych jest do chmury, a napastnicy idą z nimi w parze. Obserwuje się obecnie masowy wzrost liczby incydentów związanych z chmurą - tych bardziej i mniej zaawansowanych. Tak czy inaczej, ataki mają miejsce, a to oznacza, że organizacje muszą być czujne. Pytanie, które powinieneś sobie zadać brzmi: Czy posiadam pełny wgląd w chmurę i czy moje centrum bezpieczeństwa (SOC) jest prawidłowo skonfigurowane, aby móc odpowiedzieć na to, co się dzieje?

- **Wielkim wyzwaniem dla chmury jest powierzchnia ataku.**
- **Czy wiesz, kto teraz loguje się do Twojej infrastruktury?**
- **Kto aktualnie ma do niej dostęp?**
- **Jeżeli ktoś pobiera plik, masz pewność, że trafia do odpowiedniej osoby?**

Powinno się skupić większą uwagę na bitach i bajtach - np. przepełnienie bufora - i zrozumieć: czy to co się dzieje, powinno się dziać? Czy wstępują jakieś anomalie? Czy centrum kontroli bezpieczeństwa ma czas na badanie tych rzeczy? Musisz być w stanie zautomatyzować łatwiejsze zadania dla chmury, aby zarządzać lukami w zabezpieczeniach, tworzyć reguły dla firewalli i skupić się na wyszukiwaniu nietypowych działań oraz upewnianiu się, że wszystko jest w porządku.

Najczęstsze ataki to te, w których atakujący celuje prosto w chmurę. Zdarza się jednak, że najpierw przenika do lokalnej sieci, następnie przechodząc do chmury. Warto o tym pamiętać w 2019 roku - bardzo ważne jest monitorowanie połączeń między hybrydowym centrum danych, które znajduje się w siedzibie firmy, a chmurą.

Jednym z najważniejszych aspektów bezpieczeństwa chmurowego jest ochrona poczty elektronicznej, ze względu na wyludzanie danych. To najczęstszy sposób w jaki hakerzy atakują i nie spodziewamy się, że w 2019 roku się to zmieni. Dlatego tak ważna jest pełna widoczność i automatyzacja.



ORGANIZACJA NARODÓW ZJEDNOCZONYCH

W 2019 roku, Organizacja Stanów Zjednoczonych, zajmie się kwestią ataków sponsorowanych przez państwa, wprowadzając międzynarodowy traktat o cyberbezpieczeństwie.

Istnieje wiele przykładów domniemanych i potwierdzonych cyberataków zainicjowanych przez państwa narodowe. Stany Zjednoczone i Izrael rzekomo rozpoczęły atak o nazwie Stuxnet. Rosyjski rząd został oskarżony o atak DDoS przeciwko Estonii, na Ukrainie w trakcie wyborów oraz hackingu politycznego w Stanach Zjednoczonych. W tym samym czasie Korea Północna rzekomo zaatakowała organizacje publiczne i cywilne. Hakując Sony Pictures w ataku WannaCry, spowodowała miliardy strat.

Rosnąca liczba ofiar cywilnych dotkniętych powyższymi atakami skutkuje tym, że ONZ od 2019 roku będzie bardziej agresywnie i restrykcyjnie realizować międzynarodowy traktat o cyberbezpieczeństwie. Owa kampania ustanowi pełnoprawne i poważne konsekwencje dla Państw grających w "cyber-wojny".

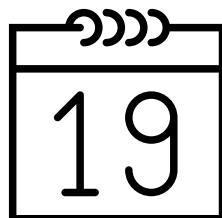


CYBER-PRZYSZŁOŚĆ W SZTUCZNEJ INTELIGENCJI

Już w 2018 roku, mieliśmy okazję poznać zaawansowane techniki uczenia maszynowego zasilanego sztuczną inteligencją. W 2019 roku, hakerzy zaczną używać sztucznej inteligencji do organizowania ukierunkowanych ataków. Wykorzystanie AI, dostarczy atakującym, zdolność przewidywania ruchów potencjalnych ofiar, co zwiększy ilość niebezpiecznych działań zawężonych do konkretnych lokalizacji i obszarów.

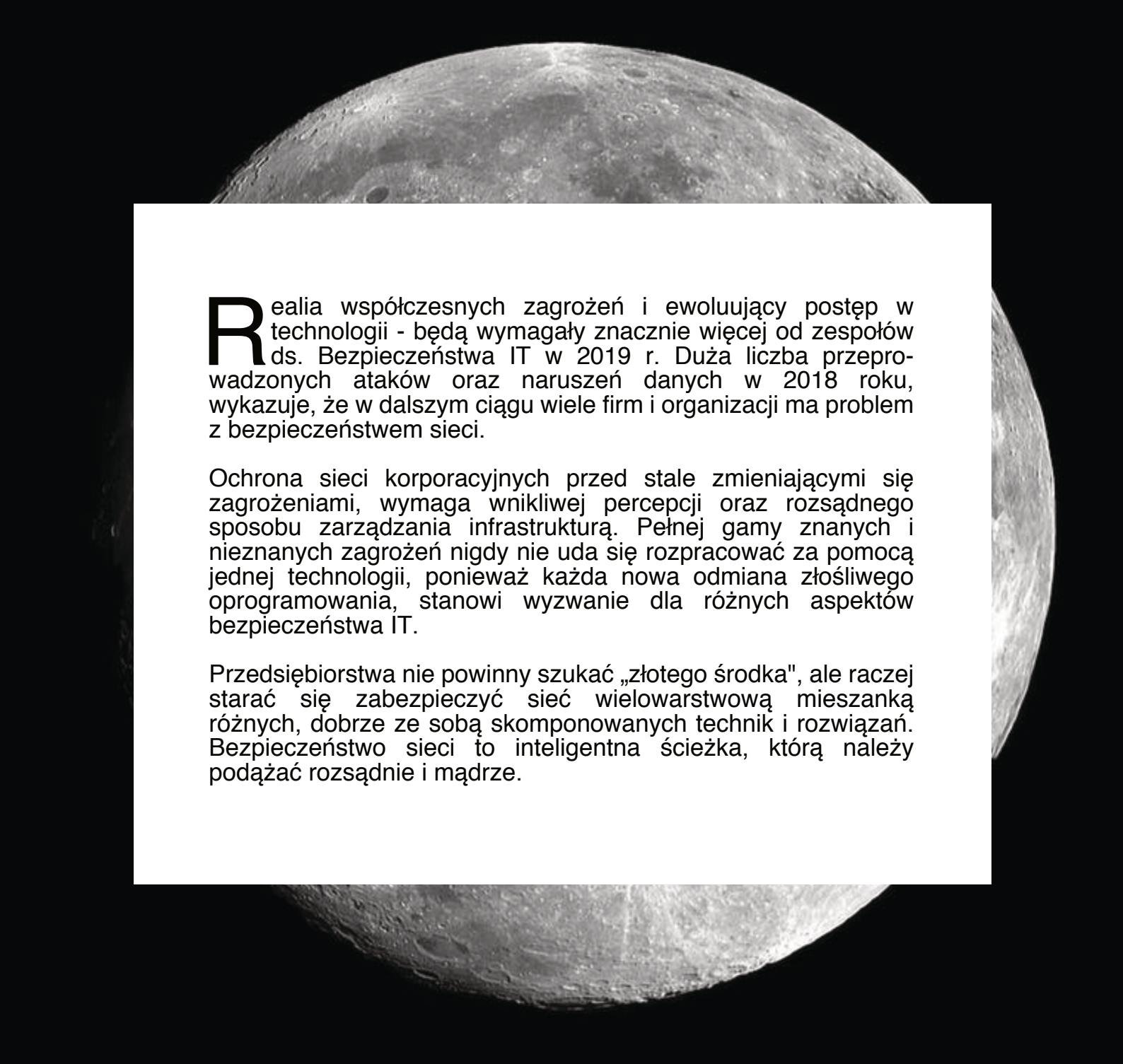
Dostawcy bezpieczeństwa będą wzmacniać defensywne techniki obrony przed sztuczną inteligencją - sami z niej korzystając! Hakerzy również nie odpuszczą. Będą wykorzystywać sztuczną inteligencję do unicestwienia jej samej. Taki futurystyczny scenariusz przewiduje się na rok 2019 jeśli chodzi o działania sztucznej inteligencji.

"Dobra AI" będzie musiała stać się jeszcze bardziej inteligentna i posłuszna. Czy powinniśmy się obawiać technologii, którą sami stworzyliśmy? W 2019 roku - według prognoz - na pewno zaczniemy się o tym przekonywać.



JAK SIĘ ZATEM CHRONIĆ W 2019 ROKU?

- powinniśmy zadbać o skuteczną ochronę przed złośliwym oprogramowaniem zaczynając od punktów końcowych. Wybierając programy antywirusowe, warto zaopatrzyć się w te, których funkcje skupiają się przede wszystkim na analizie behawioralnej i heurystycznej oraz uczeniu maszynowemu.
- do ochrony brzegu sieci powinniśmy używać inteligentnego i wielomodułowego UTM-a (najważniejsze, żeby zawierał takie moduły, jak: system IPS, APT Blocker, DLP - chroniące dane przed wyciekiem oraz TDR - Threat Detection and Response).
- powinniśmy zadbać o bezpieczeństwo poczty e-mail i programy chroniące przed spamem i atakami typu phishing.
- powinniśmy kontrolować system, przede wszystkim: aplikacje, monitorować integralność, logi.
- powinniśmy zaopatrzyć się w specjalistyczne mechanizmy wykrywania, w niestandardowe piaskownice.
- nie powinniśmy zapominać o dobrym backupie. Uniwersalna zasada -3-2-1 - mówi o tym, ile kopii zapasowych należy wykonać i gdzie je przechowywać.
- należy mieć zawsze przynajmniej trzy backupy
- należy używać dwóch różnych nośników przechowywania danych (np. w chmurze, na pendrive, na dysku zewnętrznym),
- jeden backup przechowywać zawsze poza firmą lub domem.
- zadbajmy o wieloskładnikową autoryzację i mocne hasła! 2019 rok będzie bogaty w ataki na systemy uwierzytelnienia.



Realia współczesnych zagrożeń i ewoluujący postęp w technologii - będą wymagały znacznie więcej od zespołów ds. Bezpieczeństwa IT w 2019 r. Duża liczba przeprowadzonych ataków oraz naruszeń danych w 2018 roku, wykazuje, że w dalszym ciągu wiele firm i organizacji ma problem z bezpieczeństwem sieci.

Ochrona sieci korporacyjnych przed stale zmieniającymi się zagrożeniami, wymaga wnikliwej percepcji oraz rozsądnego sposobu zarządzania infrastrukturą. Pełnej gamy znanych i nieznanych zagrożeń nigdy nie uda się rozpracować za pomocą jednej technologii, ponieważ każda nowa odmiana złośliwego oprogramowania, stanowi wyzwanie dla różnych aspektów bezpieczeństwa IT.

Przedsiębiorstwa nie powinny szukać „złotego środka”, ale raczej starać się zabezpieczyć sieć wielowarstwową mieszanką różnych, dobrze ze sobą skomponowanych technik i rozwiązań. Bezpieczeństwo sieci to inteligentna ścieżka, którą należy podążać rozsądnie i mądrze.



UL. CIESZYŃSKA 79
43-300 BIELSKO-BIAŁA

TEL. 33 472 03 18
BIURO@NETCOMPLEX.PL

ŹRÓDŁA:

Trend Micro Security Predictions for 2019

AlienVault - 2018 Threat Intelligence Report

WatchGuard's 2019 Security Predictions

Fire Eye - Facing Forward Cyber Security in 2019 and Beyond

<https://antyweb.pl/technologie-dns-anycast-na-6-kontynentach/>

<https://www.atman.pl/Cyberprzestepcy-w-2018-roku-podwoili-moc-atakow-DDoS-blog-pol-1537722575.html>

https://www.securelist.pl/analysis/7436,ataki_ddos_w_i_kwartale_2018_r.html

<https://zaufanatrzeciastrona.pl/post/uwazajcie-bo-znane-strony-www-kopia-kryptowaluty-na-waszych-komputerach/>

<https://www.theverge.com/2017/9/26/16367620/showtime-cpu-cryptocurrency-monero-coinhive>

<https://blog.malwarebytes.com/threat-analysis/2018/12/mac-malware-combines-empyre-backdoor-and-xmrig-miner/>

<https://thehackernews.com/2018/07/cryptocurrency-mining-ransomware.html>

<https://blog.malwarebytes.com/cybercrime/2018/11/malwarebytes-2019-security-predictions/>

<https://www.symantec.com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond>