Hakerzy szantażują świat

Okup i cyberkradzież własności intelektualnej najszybciej rosnącym zagrożeniem

20 miliardów dolarów strat w wyniku cyberprzestępczości ransomware. 50-60 miliardów jako koszty ataków wymierzonych w tajemnice handlowe. Częstotliwość ataków wymuszających okup - co 11 sekund. Ransomware i kradzież know-how to najszybciej rosnące zagrożenie naszych czasów – to wnioski płynące z analizy firmy Check Point.

Po koniec marca 2021 roku eksperci firmy Check Point poddali analizie atak na firmę Verkada (startup z Doliny Krzemowej), specjalizującą się w systemach monitoringu obiektów biurowych. Okazało się, że hakerzy byli w stanie uzyskać dostęp do 150,000 kodów IP kamer tej firmy. Największy problem stanowił fakt, iż hakerzy mogli przesyłać transmisje na żywo z sieci kamer każdego klienta tej firmy – takich koncernów jak Tesla, Equinox, policji stanowej, publicznego więzienia, szpitali czy placówek szkolnych. Naraziło to urządzenia, aplikacje i usługi w chmurze na potencjalną kradzież danych i własności intelektualnej.

- *Ataki ransomware wróciły w 2020 roku ze zdwojoną siłą, wywierając jeszcze większą presję na organizacjach. Szacuje się, że koszt tego typu ataków wyniósł w 2020 rok 20 miliardów dolarów, co stanowiło znaczny wzrost w stosunku do 11,5 miliarda dolarów w 2019 roku. Aby ustrzec się przed tego typu ceberprzestępczością, firmy muszą wprowadzić szeroko zakrojoną strategię zapobiegania zagrożeniom i nie polegać jedynie na systemach wykrywania i usuwania luk w systemach* – podkreśla Maya Horowitz, Dyrektor departamentu bezpieczeństwa i badań w firmie Check Point.

Potwierdzają to analizy firmy Cybersecurity Ventures, która przewiduje, że ataki ransomware na firmy będą miały miejsce co 11 sekund do 2021 roku. Jeśli weźmiemy pod uwagę konsumentów, liczba ta wzrośnie do końca 2021 roku do 5 sekund.

Jeszcze bardziej pesymistyczne wnioski płyną z raportu przygotowanego przez firmę PwC dla Komisji Europejskiej. - *Koszty cyberprzestępczości wymierzonej w tajemnice handlowe wynoszą od 50 do 60 miliardów dolarów na całym świecie i skutkują utratą konkurencyjności, miejsc pracy i zmniejszeniem inwestycji w badania i rozwój* – czytamy w raporcie „Skala i wpływ szpiegostwa przemysłowego i kradzieży tajemnic handlowych w cyberprzestrzeni" (*European Commission Report 2018)*

W konsekwencji – konkluduje raport KE - tylko w Europie zagrożonych może być co roku 289 tys. miejsc pracy w Europie a liczba ta wzrośnie w 2025 r. do miliona. Co więcej, koszty bezpośrednie to tylko około 10% kwoty, którą przedsiębiorstwa będą musiały ponieść. Pozostałe 90% kosztów zależy od skutków pośrednich i są one rejestrowane dopiero po okresie 5-6 lat.

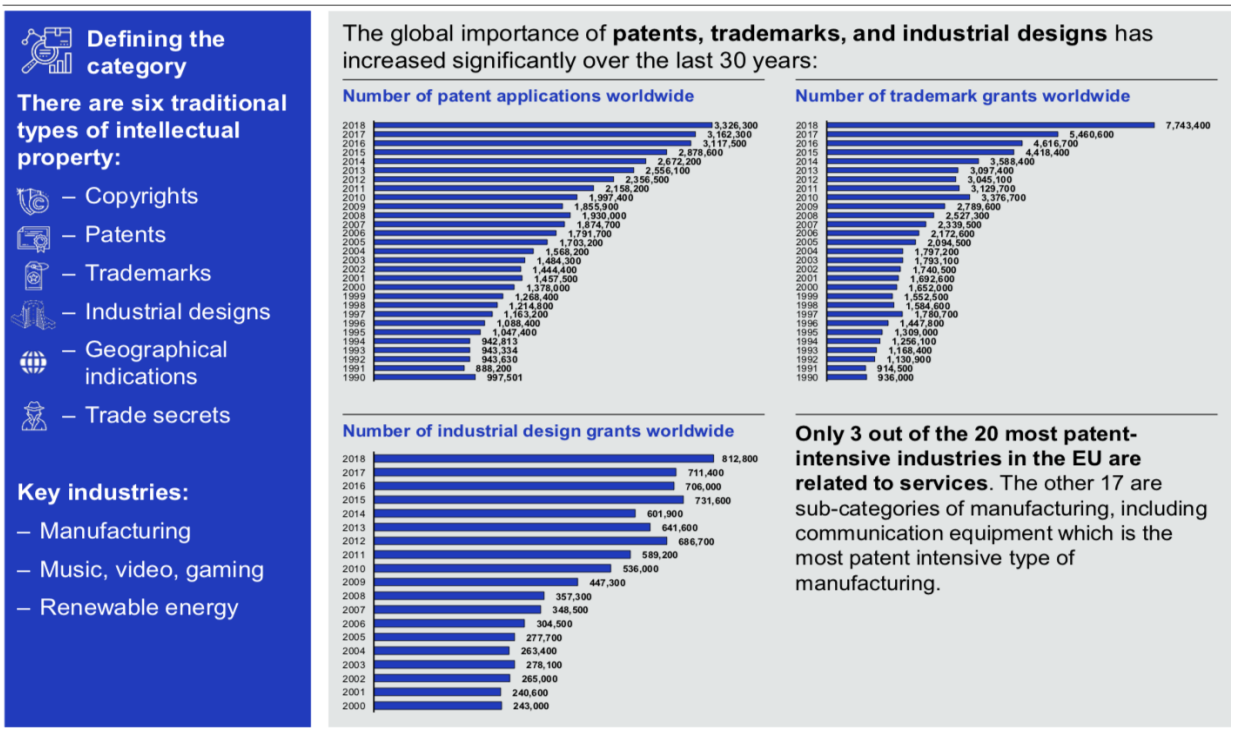
Jak podkreśla Komisja Europejska, własność intelektualna nadal jest siłą napędową organizacji. Posiadanie rozwiązania i solidnego planu zaprojektowanego w celu ochrony tych zasobów w organizacjach jest podstawowym sposobem zapobiegania kradzieży danych.

Eksperci nie mają wątpliwości: ataki wymierzone we własność intelektualną firm będą się zdarzać coraz częściej. Tylko w USA zagraniczna kradzież amerykańskiej własności intelektualnej kosztuje obecnie od 225 do 600 miliardów dolarów rocznie. Znaczna część tego jest wynikiem cyberprzestępczości.

Własność intelektualna (*Intellectual Property, IP*) – co to jest?

Własność intelektualna obejmuje prawo autorskie i własność przemysłową. W gospodarce opartej na wiedzy własność intelektualna jest jednym z głównych czynników pozwalających stworzyć przewagę konkurencyjną i decydować o sukcesie rynkowym. Z drugiej strony, brak ochrony w zakresie własności przemysłowej może spowodować nieodwracalne szkody. Natomiast zapewnienie odpowiedniej ochrony znaków towarowych, wynalazków i wzorów nie tylko pozwala zamienić pomysł w prawo o rzeczywistej wartości rynkowej, ale umożliwia powstrzymanie potencjalnych naruszeń takiego prawa. Niezależnie od korzyści płynących z budowy pozycji rynkowej, ochrona praw własności przemysłowej zapewnia również istotne korzyści podatkowe: prawa własności intelektualnej, będące niematerialnymi składnikami majątku, mogą być przedmiotem amortyzacji i stąd obniżają zyski podlegające opodatkowaniu; licencjonowanie może być źródłem przychodów; może również stanowić instrument generowania kosztów.

W opinii firmy KPMG, całkowita wartość własności intelektualnej jest znacząca i rośnie w większości części świata, zwłaszcza w Azji (w Chinach). Przemysł wytwórczy (szczególnie związany z technologią) jest głównym punktem dostępowym dla aplikacji związanych z własnością intelektualną. Większość głównych krajów OECD wydaje 2-3% swojego PKB na badania i rozwój, co jest dobrym wskaźnikiem całkowitej wartości tajemnic handlowych (tylko jeden rodzaj własności intelektualnej). Całkowity koszt sporów sądowych w zakresie praw własności intelektualnej nadal rośnie, a sprawy sądowe stają się coraz bardziej złożone i kosztowne. Całkowite straty powstałe w wyniku kradzieży własności intelektualnej są mierzone w dziesiątkach miliardów funtów i szybko rosną.



Source: World Intellectual Property Organization; Statista; KPMG analysis

Własności intelektualne – jedne z najcenniejszych, łatwych do policzenia dóbr niematerialnych
Źródło wykresów: KPMG

Kradzież IP – kiedyś i dziś

Jak zauważają eksperci firmy Deloitte dawniej kradzież własności intelektualnej (IP) przybierała postać przejmowania dokumentów, dysków komputerowych i protokołów przez niezadowolonych pracowników. Niewielka liczba osób z fizycznym dostępem ograniczała pulę podejrzanych, często czyniąc taką kradzież ryzykowną. Obecnie, w cyfrowym świecie, złodzieje IP mogą działać z dowolnego miejsca, zachowując względną anonimowość, co sprawia, że pula potencjalnych podejrzanych jest zarówno szeroka, jak i głęboka. Do sprawców mogą należeć obecni i byli pracownicy, konkurenci, hakerzy kryminalni oraz podmioty z innych państw. Motywacją mogą być pobudki finansowe lub chęć pozyskania sławy w sieci.

Hakerzy sprawdzają możliwości monetyzacji wirtualnego łupu. Wobec firm notowanych na rykach finansowych, mogą podejmować próby zastraszania firmy w oczach inwestorów. Wobec firm działających w UE, mogą straszyć karami związanymi z RODO. Ale prawdziwe zagrożenie stanowi utrata poufnych danych, kodów, patentów, których strata może zaważyć na przyszłości poszkodowanego przedsiębiorstwa.

Bardzo jaskrawym przykładem skutków ataku hakerów na własność intelektualną przedsiębiorstwa była głośna sprawa polskiej spółki CD Projekt Red. Pokazała ona, że nawet największe firmy technologiczne mogą paść ofiarą ataku typu ransomware (wymuszenie okupu).

Atak cyberprzestępców typu *ransomware* to przenikanie złośliwego oprogramowania do wewnętrznej sieci przede wszystkim w wyniku błędu człowieka. Codziennie pracownicy są bombardowani przez różnego rodzaju ataki socjotechniczne: wiadomości e-mail od usługodawców i partnerów biznesowych (spear phishing), SMS od podszywających się pod kuriera (smshing), wiadomości z *podstawionych kont* zarządu lub osób decyzyjnych (spoofing i podszywanie się). Hakerzy nie odpuszczają również największym tego świata – często prezesi i właściciele firm padają ataków typu whaling (Jeff Bezos prezes Amazon) – włamań na ich konta Twitter, FB. Ataki typu whaling są stosunkowo trudne do wykonania, ale przynoszą hakerom największe korzyści. Prezesi firm i członkowie zarządu są uprzywilejowani w kwestii dostępu do danych: w przeciwieństwie do średniego szczebla pracowników, nie obejmuje ich wielopoziomowa struktura dostępu do informacji. Skompromitowanie urządzenia lub konta prezesa jest więc „strzałem w dziesiątkę".

Ataki socjotechniczne i inżynieria społeczna okazują się skuteczne nie tylko w uzyskiwaniu dostępu do sieci korporacyjnych. Hakerzy czerpią korzyści z wykorzystania autorytetu zhakowanej osoby – tak, jak się to wydarzyło u szefa Amazonu. W połowie 2020 roku specjaliści Check Point zauważyli, że wiele znanych kont na Twitterze zostało przejętych w ramach kampanii, która wydawała się być atakiem socjotechnicznym na niektórych pracowników Twittera. Obejęła on konta Baracka Obamy, Joe Bidena, Elona Muska, a także oficjalne konta Uber, Apple i giełd kryptowalut. Hakerzy wykorzystali autorytet osób takich jak Elon Musk, Barack Obama czy Joe Biden, aby w ciągu kilku minut zarobić 115 tysięcy dolarów. Hakerzy dostali się do kont Twittera znanych osób i zachęcali do wpłaty BitCoinów na podany adres wymyślonej organizacji o nazwie „CryptoForHealth", w celu pomnożenia pieniędzy. Oferta została przedstawiona jako akcja charytatywna, a sam autorytet właścicieli kont Twittera wystarczył, aby internauci wpłacili pieniądze.

- *Atak na konta Twittera pokazuje, że w dzisiejszym świecie - przy rosnącej liczbie ataków i przypadków utraty danych - organizacje mają niewielki wybór i muszą pilnie podjąć działania w celu ochrony poufnych danych* - napisała firma bezpieczeństwa Check Point w poście na swoim blogu.

- *Poufne dane pracowników i klientów, dokumenty prawne i własność intelektualna są codziennie ujawniane niepożądanym stronom*. *W rzeczywistości co najmniej 30% naruszeń dokonywanych jest przez osoby wewnątrz organizacji* – czytamy z kolei w raporcie Check Point *Securing the New Normal 2020*.

Badanie przeprowadzone przez tę firmę w 2020 roku wykazało, że dla ponad 75% firm na świecie największym zmartwieniem jest wzrost liczby ataków cybernetycznych, zwłaszcza ataków typu phishing i inżynierii społecznej. 51% stwierdziło, że problemem były ataki na niezarządzane domowe punkty końcowe, a następnie ataki na urządzenia mobilne pracowników (33%).

Szpiegostwo przemysłowe. Szczepionki na COVID-19 celem ataków

Mając na uwadze statystyki raportu KPMG (najbardziej narażone sektory na ataki IPP i ransomware to przemysł muzyczny, technologiczny i energetyczny) nie może dziwić wzrost liczby ataków o charakterze szpiegostwa technologicznego w 2020 roku i kolejnych latach…

W Europie przykładem mogą być Niemcy. W połowie 2020 roku Arne Schönbohm, szef niemieckiego Federalnego Urzędu Bezpieczeństwa Teleinformatycznego (BSI), przyznał, że zagrożenie dla niemieckich firm farmaceutycznych i producentów szczepionek jako wysokie. Jednocześnie potwierdził, że BSI dowiedziało się o kilku atakach na firmy farmaceutyczne oraz instytuty badawcze lub uniwersytety. - *Nadal istnieje ryzyko ukierunkowanych ataków na takie instytucje* - podkreślał prezes BSI. Urząd wystosował ostrzeżenie dla niemieckich przedsiębiorstw.

Obawy o bezpieczeństwo niemieckich instytucji podzielił Niemieckie Urząd Ochrony Konstytucji. W swoim raporcie stwierdził, że - *obce mocarstwa używają wszelkich dostępnych środków i sposobów ukrytego działania przeciwko Republice Federalnej Niemiec, aby realizować swoje interesy. Szczególnie służby wywiadowcze Federacji Rosyjskiej i Chińskiej Republiki Ludowej rozwijają działalność szpiegowską w cyberprzestrzeni przeciwko niemieckim organom władzy*.

Choć dotychczas nie było oficjalnego zgłoszenia do niemieckich organów ścigania przypadku udanego ataku cybernetycznego na firmę farmaceutyczną, przypadek firmy AstraZeneca i włamań do systemów tej firmy pokazuje, jak niebezpieczna jest sytuacja.

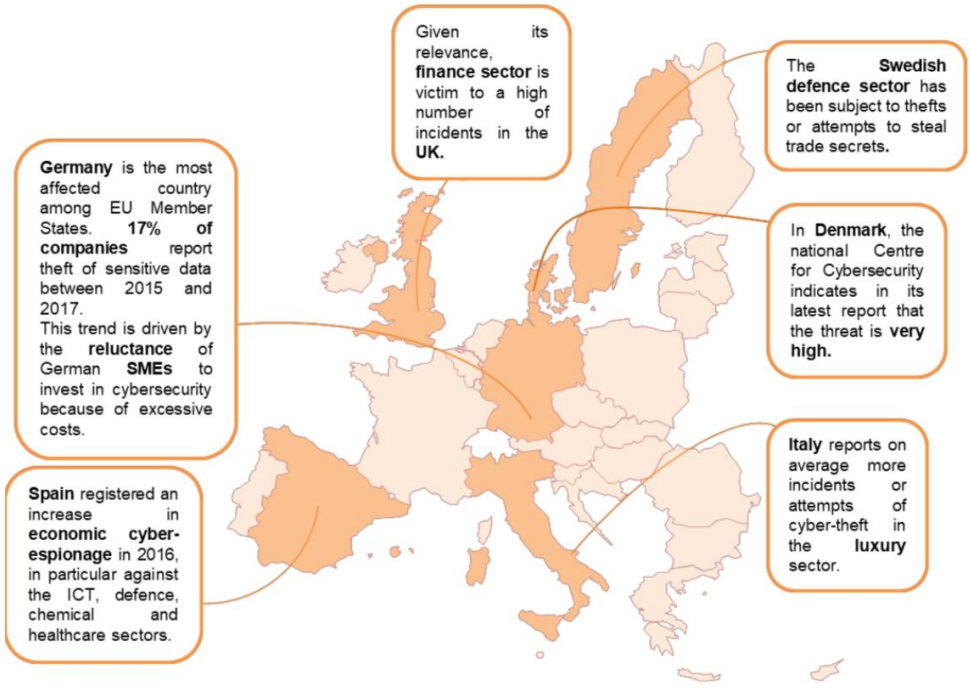
Po koniec 2020 roku świat obiegła informacja o ataku na konta e-mail pracowników brytyjsko-szwedzkiego producenta szczepionki AstraZeneca. Hakerzy dołączyli do swoich maili z ofertami pracy złośliwe wirusy, za pomocą których chcieli uzyskać dostęp do komputerów twórców szczepionki.

Tymczasem już w lipcu 2020 roku wywiad USA, Kanady i Anglii wskazywały rosyjskich hakerów jako źródło ataków na organizacje zaangażowane w opracowywanie szczepionek na COVID-19. W opinii British National Cyber Security Centre (NCSC), grupa hakerów, działająca pod kryptonimem APT29, miała na celu „kradzież cennej własności intelektualnej". APT29, znana również jako „Cozy Bear", według NCSC działa częściowo w ramach rosyjskich służb specjalnych.

Działania służb wywiadowczych państw nie dziwią ekspertów. Mikko Hypponen Fiński, ekspert ds. bezpieczeństwa cybernetycznego zasadniczo nie jest zaskoczony szpiegostwem przemysłowym na zlecenie państwa. - *Misją agencji wywiadowczych jest ochrona swoich krajów przed atakiem* – powiedział w wywiadzie dla niemieckiej agencji Deutsche Welle w 2020 roku. - *Nic więc dziwnego, że agencje wywiadowcze starają się zdobyć przewagę, która pomogłaby im obronić swój naród także przed pandemią* – dodał.

Chęć przejęcia danych o szczepionkach popchnęła cyberprzestępców do ataku na Europejską Agencję Leków (EMA). - *EMA stała się celem cyberataku. Agencja szybko wszczęła pełne dochodzenie, w ścisłej współpracy z organami ścigania i innymi właściwymi podmiotami* – informowała Europejska Agencja Leków. Kilka godzin później na jaw wyszło, że w trakcie ataku wykradzione zostały dokumenty dotyczące szczepionki przeciwko COVID-19 stworzonej przez firmy Pfizer i BioNTech.

Uważa się, że metody zastosowane w tym ataku wskazywały na Koreę Północną, Iran, Wietnam, Chiny i Rosji, jako autora ataków.



Geograficzne rozmieszczenie incydentów – dane za PwC „Skala i wpływ szpiegostwa przemysłowego i kradzieży tajemnic handlowych w cyberprzestrzeni'' *(European Commission Report 2018)*

Ciekawe spostrzeżenia dotyczące geograficznego rozmieszczenia incydentów hakerskich na własność intelektualną w Europie zawiera przywołany wcześniej raport PwC z 2018 roku. Okazuje się, że ataki są bardzo zróżnicowane w całej Europie. Na przykład we Włoszech najbardziej podatny jest przemysł luksusowy, biorąc pod uwagę solidną reputację kraju w tej dziedzinie, podczas gdy w Wielkiej Brytanii hakerzy celowali najczęściej w sektor finansowy. W Danii różne firmy informatyczne padają ofiarą kradzieży wrażliwych danych. W Holandii firmy z różnych sektorów przemysłu, takich jak energetyka, zaawansowane technologie i chemia, najbardziej cierpią z powodu cyberszpiegostwa.

Koszty cyberataków na własność intelektualną i dla okupu

Ransomware pozostaje najbardziej dominującym zagrożeniem, ponieważ przestępcy zwiększają presję, grożąc publikacją danych, jeśli ofiary nie zapłacą - podkreśla Europol w raporcie IOCTA 2020.

Koszty ataków ransomware na własność intelektualną rosną. Firma Check Point szacuje, że w 3 kwartale 2020 r. prawie połowa wszystkich przypadków ransomware obejmowała zagrożenie ujawnieniem skradzionych danych, a średnia płatność okupu wyniosła ponad 230 tys. dolarów – co stanowiło wzrost o 30% w porównaniu z drugim kwartałem 2020 r.

Tymczasem całkowite, globalne koszty cyberprzestępczości będą rosły o 15 procent rocznie w ciągu najbliższych pięciu lat i osiągają poziom 10,5 biliona dolarów rocznie do 2025 roku, w porównaniu z 3 bilionami dolarów w 2015 roku – twierdzi Cybersecurity Ventures.

O skali zjawiska w USA świadczyć może informacja ujawniona w 2018 roku dziennikowi Wall Street Journal przez agenta FBI, sugerująca, że każdy obywatel amerykański powinien spodziewać się, że wszystkie jego dane (informacje umożliwiające identyfikację) zostały skradzione i będą wykorzystane w Dark Web. Według niektórych szacunków rozmiar Dark Net (przestrzeń nie jest indeksowana ani dostępna dla wyszukiwarek) jest nawet 5000 razy większa niż sieci ogólnodostępnej.

Niniejszy raport został opracowany przez firmę Bellini i Check Point Software Technologies (Kwiecień 2021), na podstawie badań i analiz firmy Check Point Research oraz danych na temat rynku.