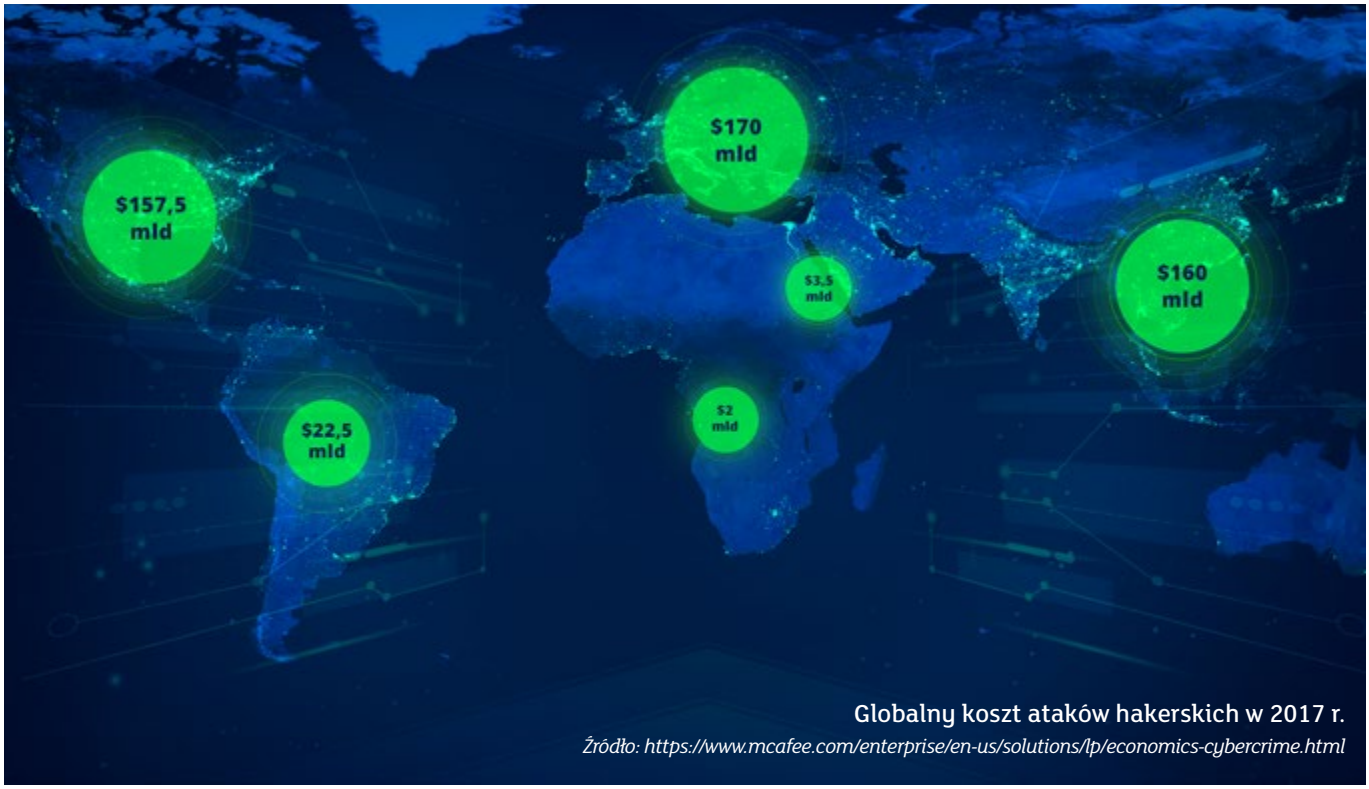


Globalny koszt ataków hakerskich w 2017 r.
Źródło: https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

Cyberbezpieczeństwo

Z raportu KPMG „Barometr cyberbezpieczeństwa”[1] wynika, że w 2018 roku skutki przestępczości on-line dotknęły 68% badanych firm. 25% przedsiębiorstw odnotowało wzrost prób ataków cybernetycznych. Jednocześnie ponad połowa firm ma opracowane procedury na wypadek ataku hakerskiego. Cyberataki stają się więc, coraz powszechniejszym zjawiskiem, które naturalnie prowadzi do poszukiwania „antidotum” – cyberbezpieczeństwa.

Przenoszenie się usług, rozrywki czy życia gospodarczego do internetu przestało być scenariuszem filmu science fiction. Dzieje się to na naszych oczach. Rośnie wykorzystanie e-commerce, bankowości mobilnej, coraz więcej spraw urzędowych możemy załatwić zdalnie.

Trend ten przybrał na sile w czasie globalnej pandemii. Do tak istotnych argumentów digitalizacji, jak niższy koszt czy wygoda, doszła jeszcze kwestia bezpieczeństwa uczestników życia gospodarczego.

Zjawisko wirtualizacji niesie ze sobą jednak również ryzyka. Życie on-line nie jest pozbawione zagrożeń ze strony przestępców. Bandyci zamienili jedynie kominiarki i pistolety na klawiatury, wirusy i socjotechniki.

Jak wyłączyć lotnisko i metro?

Wyraźnym przykładem, jak szeroki może być zasięg działań hakerskich, są wydarzenia na Ukrainie w 2017 roku. Grupa cyberprzestępców sparaliżowała najważniejsze instytucje państwowe i prywatne. Rządowa sieć komputerowa, łącznie z lotniskiem i metrem w Kijowie, przestała działać, co stanowiło bezpośrednie zagrożenie dla zdrowia i życia mieszkańców. Atak odbył się dzień przed ukraińskim Dniem Konstytucji 27 czerwca, a usuwanie jego skutków potrwało aż do pierwszych dni lipca.

Co gorsza, nie był to pierwszy atak cybernetyczny na Ukrainę. Dwa lata wcześniej wirus zakłócił przesyłanie energii elektrycznej. Winą za te wydarzenia została obarczona Rosja,

z którą Ukraina prowadzi wojnę. Pokazuje to wyraźnie, że w XXI wieku efektem konfliktów mogą być również ataki w sferze „wirtualnej".

Wojny cybernetyczne

Innym przykładem ataku na infrastrukturę całego kraju była hakerska akcja przeciwko Estonii w 2007 roku. Przestał działać wówczas system bankowy oraz łączności. Również tu oskarżenia skierowano przeciwko Rosji, ale na potwierdzenie tego nie zostały przedstawione żadne dowody. Atak poprzedzały jednak burzliwe negocjacje z Rosją o usunięcie z centrum Tallina pomnika upamiętniającego żołnierzy ZSRR i protesty mniejszości rosyjskiej. Cybernetyczny paraliż trwał kilka dni. Był to pierwszy w historii zmasowany atak przeciwko suwerennemu państwu. Od tego momentu kraje tworzą systemy obrony cyberprzestrzeni i pracują nad możliwością przeprowadzenia, w razie konieczności, ofensywy.

O tym, że współczesna wojna toczy się także w wirtualnym świecie mogą świadczyć chociażby ujawnione materiały holenderskich służb specjalnych. Te włamały się do sieci rosyjskiej grupy hakerskiej, działającej w ramach wywiadu wojskowego[2].

Wskazuje to na konieczność inwestowania przez rządy zarówno w systemy obrony cyberprzestrzeni, jak i systemy ofensywy wywiadu cyfrowego. Cyberbezpieczeństwo jest więc dziś jednym z największych wyzwań nie tylko dla firm, ale również całych gospodarek.

Ile to wszystko kosztuje?

Petya, CryptoLocker, Locky, Bad Rabbit, TeslaCrypt, Stuxnet, ILOVEYOU czy WannaCry to nazwy, które spędzały sen z powiek zarządom międzynarodowych korporacji. Petya

(wirus odpowiedzialny za paraliż Ukrainy w 2007 roku) kosztował niektóre globalne firmy kilkaset milionów dolarów[3].

Mniej znany atak – WannaCry – mógł wywołać jeszcze większe straty. Zainfekował dziesiątki tysięcy komputerów, blokując na nich dane, a hakerzy, wraz z upływem czasu, żądali coraz wyższego okupu. Atak objął nawet szpitale, jego zasięg miał charakter globalny.

Z obliczeń firmy Symantec[4], światowego lidera w dostarczaniu oprogramowania antywirusowego, wynika, że tylko w przypadku osób prywatnych w 2017 roku koszty ataków hakerskich wyniosły 172 mld USD, a przeciętna ofiara straciła 142 USD. Jeśli uwzględnimy straty przedsiębiorstw, wartości te będą kilkukrotnie wyższe. Firma szacuje, że dziennie dochodzi do miliona ataków, a 65% z nich stanowią zainfekowane maile.

Co ciekawe, to nie USA dzierży niechlubny tytuł lidera, jeśli chodzi o cyberprzestępczość. 25% wszystkich ataków na świecie ma miejsce w Chinach. Na drugim miejscu jest USA z blisko 10% udziałem, a trzecia, minimalnie dalej, jest Brazylia.

Tylko w przypadku osób prywatnych w 2017 roku koszty ataków hakerskich wyniosły

172 mld USD

Dziennie dochodzi do miliona ataków, a 65% z nich stanowią zainfekowane maile.

Według McAfee, globalny koszt ataków hakerskich przekraczał w 2018 roku 600 mld USD, co stanowi blisko 1% globalnego PKB[5]. Inne ośrodki szacują, że straty z tytułu cyberprzestępczości tylko w USA przekraczają już znacznie 600 mld USD[6]. Niestety wiele wskazuje na to, że trend ten pozostanie wzrostowy. Dekadę wcześniej koszty związane z cyberprzestępczością szacowano na ok. 300 mld USD.

Kto na tym traci a kto zyskuje?

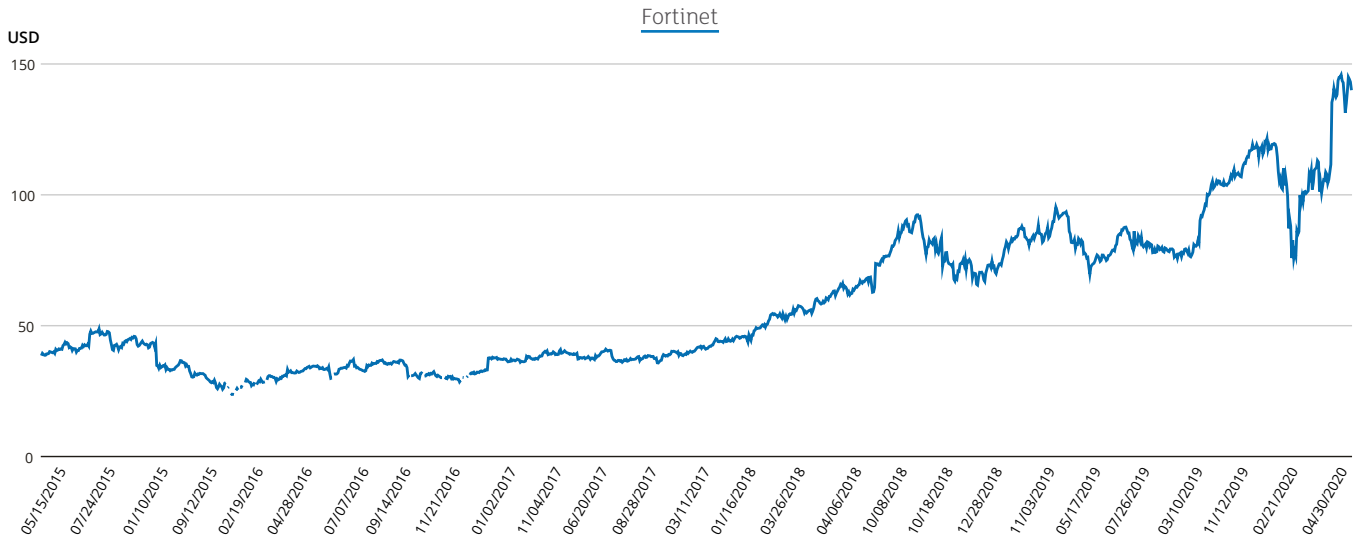
Blisko połowa firm ponosi straty finansowe w wyniku ataków cybernetycznych, a 85% konsumentów twierdzi, że nie zamierza korzystać z usług firmy, która nie jest w stanie zapewnić odpowiedniego bezpieczeństwa danych.[7] Zagrożenie jest więc zbyt duże i zbyt prawdopodobne, by przedsiębiorstwa mogły pozwolić sobie na lekceważenie go. Dlatego rosną budżety przeznaczone na cyberbezpieczeństwo.

Jeszcze kilka lat temu średnia wartość środków przeznaczanych na ten cel stanowiła poniżej jednego procenta wszystkich wydatków przedsiębiorstw. Dziś coraz częściej znacznie go przekracza.

Raport KPMG „Barometr cyberbezpieczeństwa" wskazuje, że 70% przedsiębiorstw korzysta z outsourcingu usług bezpieczeństwa. Popyt na usługi firm specjalizujących się w cyberbezpieczeństwie wynika ze skomplikowania tej materii i z konieczności ciągłego udoskonalania procesów. Charakter zagrożeń zmienia się bowiem dynamicznie.

Spółka Fortinet

Jedną z firm dostarczających oprogramowanie antywirusowe jest Fortinet. Ta międzynarodowa korporacja z siedzibą w Dolinie Krzemowej, notowana na Nasdaq-u, jest jednym z największych światowych producentów oprogramowania antywirusowego. Spółka sprzedaje swoje rozwiązania w 30 krajach, a jej produkty są przeznaczone zarówno dla małych firm, jak i międzynarodowych korporacji. Z jej usług korzystają również instytucje rządowe. Licząc od 2014 roku, średnioroczny wzrost sprzedaży spółki wynosi 26%. W 2018 roku zwiększył się on o 20% i wyniósł 1.8 miliarda dolarów, a wzrost odnotowano na wszystkich rynkach. Sama spółka posiada przeszło miliard dolarów gotówki, co zapewnia odpowiedni bufor bezpieczeństwa. Dobrą sytuację firmy i świetne perspektywy całej branży obrazuje wykres notowań jej akcji. Marcowe załamanie związane z pandemią koronowirusa bardzo szybko zostało odrobione. Obecnie ceny akcji Fortinetu kreślą nowe szczyty wszech czasów. Co istotne, notowania spółki na przestrzeni ostatniej dekady rosną niemal w tempie wykładniczym.

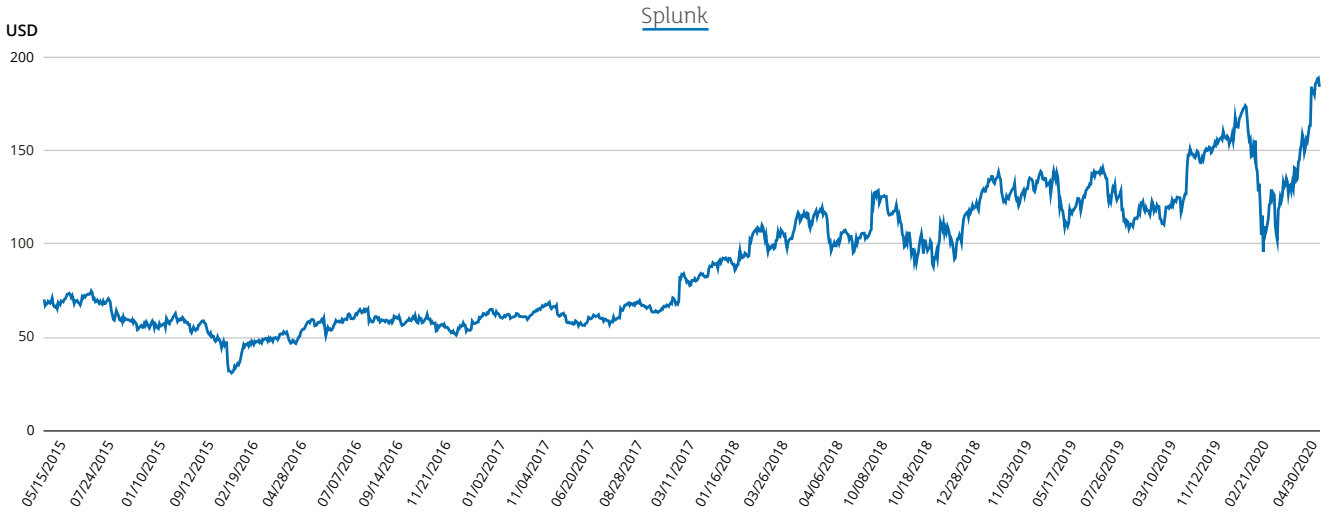


Źródło: Bloomberg

Spółka Splunk

Przykładem innej firmy z tej branży jest Splunk. To amerykańska korporacja, również wywodząca się z Kalifornii, która tworzy oprogramowanie do wyszukiwania zagrożeń w sieci. Firma koncentruje się na budowaniu aplikacji analizujących duże zbiory danych. Korporacja ma klientów na całym świecie i współpracuje z takimi gigantami jak np. Microsoft. W ostatnich latach przychody spółki rosły bardzo dynamicznie i w 2015-2019 zwiększyły się o 300%. W 2019 roku wyniosły one 1.8 miliarda USD i wzrosły o 38% r/r. Akcje spółki zdążyły już też odrobić załamanie związane z pandemią koronawirusa.

Spółki Fortinet i Splunk mają największe udziały w portfelu funduszu ETF z tematu Cyberbezpieczeństwo w mBanku



Źródło: Bloomberg

Skład portfela (Top 10) na dzień 31.12.2019

FORTINET	4,23%
SPLUNK	3,83%
FIREEYE	3,72%
RAPID 7	3,64%
PALO ALTO NETWORK	3,45%
CYBER ARK SOFTWARE	3,44%
TREND MICRO	3,41%
NORTONLIFELOCK	3,32%
QUALYS	3,29%
RADWARE	3,22%
POZOSTAŁE	64,45%

> To tylko dwie spółki spośród kilkuset, które specjalizują się w dziedzinach związanych z cyberbezpieczeństwem.

Spółki Fortinet i Splunk mają największe udziały w portfelu funduszu ETF z tematu Cyberbezpieczeństwo w mBanku.

Ryzyka dla branży

Dla równowagi, należy zwrócić również uwagę na ryzyka dla całej branży, mimo że wydają się minimalne. Marzeniem ściętej głowy jest to, by cyberprzestępcy porzucili dotychczasowe zajęcie. Poziom zabezpieczeń nie osiągnął też jeszcze pułapu, przy którym ich starania stałyby się bezużyteczne. Największe zagrożenie dla tej branży wiąże się z ryzykiem głębokiej i przedłużającej się recesji. Może ona uszczuplić budżety przedsiębiorstw, a w dalszej kolejności ich wydatki na infrastrukturę IT.

Szybka popularyzacja internetu przyniosła ze sobą równie gwałtowną falę przestępczości cybernetycznej. Jedyną odpowiedzią na to mógł być rozwój cyberbezpieczeństwa. Tworzenie zabezpieczeń stało się krytyczne zarówno dla rządów, międzynarodowych korporacji, banków, jak i niewielkich firm.

autor: Rafał Sadoch

1. KPMG, Barometr cyberbezpieczeństwa. W obronie przed cyberatakami, Kwiecień 2019; 2. Holenderskie służby wywiadowcze złapały hakerów z Rosji na gorącym uczynku, gazetaprawna.pl, 26.01.2018; 3. NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million, forbes.com, 16.08.2017; 4. Norton Cyber Security Insights Report Global Results 2017; 5. The Economic Impact of Cybercrime— No Slowing Down, McAfee, Luty 2018; 6. https://www.forgerock.com/about-us/press-releases/forgerock-us-consumer-data-breach-report-data-breaches-cost-654-billion; 7. PwC US, Protect.me Survey, 2017