20 LECIE 1998-2018

MAJKOWSKI BROKERS
GRUPA FST

Ryzyka **cybernetyczne**

Jesteśmy kluczem
DO TWOJEGO BEZPIECZEŃSTWA

Czym są **ryzyka cybernetyczne?**

Ryzyka cybernetyczne to ryzyka związane z użytkowaniem systemów IT. Dotyczą one praktycznie każdego urządzenia, które choćby pośrednio połączone jest z internetem. Smartfony, tablety, komputery, systemy sterowania przemysłowego i każde inne urządzenie czy system mający połączenie internetowe jest zagrożone.

Co mi grozi?

Zależnie od przyjętej przez cyberprzestępców metody skutkiem działania może być:

KRADZIEŻ DANYCH OSOBOWYCH

Kradzież danych osobowych, które znajdują się w systemach komputerowych. Takie zdarzenie do niedawna nie miało dużych konsekwencji. To jednak zmienia się w bieżącym roku za sprawą wejścia w życie Rozporządzenia o Ochronie Danych Osobowych (RODO). Na mocy RODO sankcje za niezabezpieczenie danych zostaną zaostrzone, a kara jaką może nałożyć organ nadzoru wynosić może nawet 20 milionów euro.

KONIECZNOŚĆ WYPŁATY ODSZKODOWANIA

Konieczność wypłaty odszkodowania, na skutek wycieku danych, nad którymi w momencie wycieku tracimy kontrolę ale nie odpowiedzialność za nie. Poszkodowany może zwrócić się do nas z roszczeniem o odszkodowanie. Przykładem takiej sytuacji może być kazus wycieku danych z jednego z polskich banków. Poszkodowana na skutek ujawnienia jej danych spotkała się z uporczywym nękaniem ze strony osób, które uzyskały dostęp do tych danych a sąd przyznał jej 10 000 zł odszkodowania na skutek jej pozwu przeciwko bankowi.

ZAINFEKOWANIE ZŁOŚLIWYM OPROGRAMOWANIEM

Zainfekowanie złośliwym oprogramowaniem, które nie ujawniając żadnych zauważalnych oznak będzie np. zmieniało numery kont bankowych w wysyłanych przelewach. Na skutek takiego ataku możliwa jest sytuacja przelania pieniędzy na konto przestępców, zamiast na konto kontrahenta nie zdając sobie z tego sprawy.

ATAK ZAKŁÓCAJĄCY PRACĘ SYSTEMÓW

Atak zakłócający pracę systemów. Może on powodować wyłączenie, włączenie, zmianę trybu pracy urządzeń czy systemów sterowania. Dotknięty takim atakiem system produkcyjny może zostać trwale uszkodzony a przestój w działalności spowodować utratę zysku firmy.

ZASZYFROWANIE DANYCH

Zaszyfrowanie danych przechowywanych na dysku i żądanie opłacenia okupu w zamian za kod odblokowujący. Korzystanie z komputera zaatakowanego w taki sposób jest niemożliwe aż do odblokowania. Niestety nie zawsze jest to możliwe a dane zostają bezpowrotnie utracone. Sytuacja taka powoduje realne przestoje w funkcjonowaniu przedsiębiorstwa, gdyż uniemożliwia chociażby kontakt z kontrahentami, dostęp do bieżących danych, faktur itp.

Czy zagrożenie **mnie dotyczy?**

W dobie powszechnego dostępu do internetu atak na nasz system nie musi być atakiem przeprowadzanym bezpośrednio na nas. Zainfekowany plik może znaleźć się w każdym miejscu w cyberprzestrzeni.

Wirusy infekujące sieci na całym świecie i na globalną skalę to dzisiejszy przykry standard. Petya, NotPetya, WannaCry to przykłady infekcji systemów komputerowych, które w ostatnich miesiącach i latach doprowadziły do ogromnych strat takich gigantów jak Maersk (operator logistyczny) czy Merck (gigant farmaceutyczny). Z całą pewnością można powiedzieć, że zagrożenie dotyczy każdego.

Jak zabezpieczyć się na ewentualność **ataku?**

Przede wszystkim należy pamiętać aby korzystać z oprogramowania aktualnego, z dostępnym wsparciem producenta a także oprogramowania antywirusowego. Posiadanie polityki bezpieczeństwa w zakresie cyber-bezpieczeństwa to także dobre rozwiązanie. Kolejnym czynnikiem mogącym zmniejszać ryzyko stania się ofiarą cyberataku będzie odpowiednie przeszkolenie pracowników w tym zakresie. Niestety takie zabezpieczenia mogą okazać się niewystarczające. Nie ma rozwiązania, które zapewni 100% bezpieczeństwa

PRZYKŁADY **DZIAŁANIA CYBERPRZESTĘPCÓW**

1

„Ransomware Petya unieruchomił całą sieć szczecineckiego Kronospanu, wcześniej blokując jego oddział między innymi na Ukrainie oraz w Niemczech. Nie działa sieć komputerowa ani czytniki kart. Pracownicy nie mają dostępu do kont e-mail."

https://szczecinek.com/artykul/petya-zada-okupu-od/258519

2

„W wyniku zakłócenia funkcjonowania systemów teleinformatycznych grupy kapitałowej Inter Cars nastąpiła przerwa w działaniu systemów sprzedażowych spółki i jej podmiotów zależnych, co zostało prawdopodobnie spowodowane międzynarodowym atakiem hakerskim. - podał Inter Cars."

https://silesion.pl/wirus-petya-atakuje-padly-systemy-sprzedazowe-inter-cars-28-06-2017

3

W czerwcu 2017 roku ransomware NotPetya zainfekował systemy komputerowe firm w USA i Europie. Jedną z ofiar był kopenhaski gigant żeglugowy AP Moller-Maersk, który odpowiada za około jedną piątą światowego transportu towarowego. Operacje na terminalach Maersk w czterech różnych krajach zostały sparaliżowane, powodując opóźnienia i zakłócenia, które trwały tygodnie.

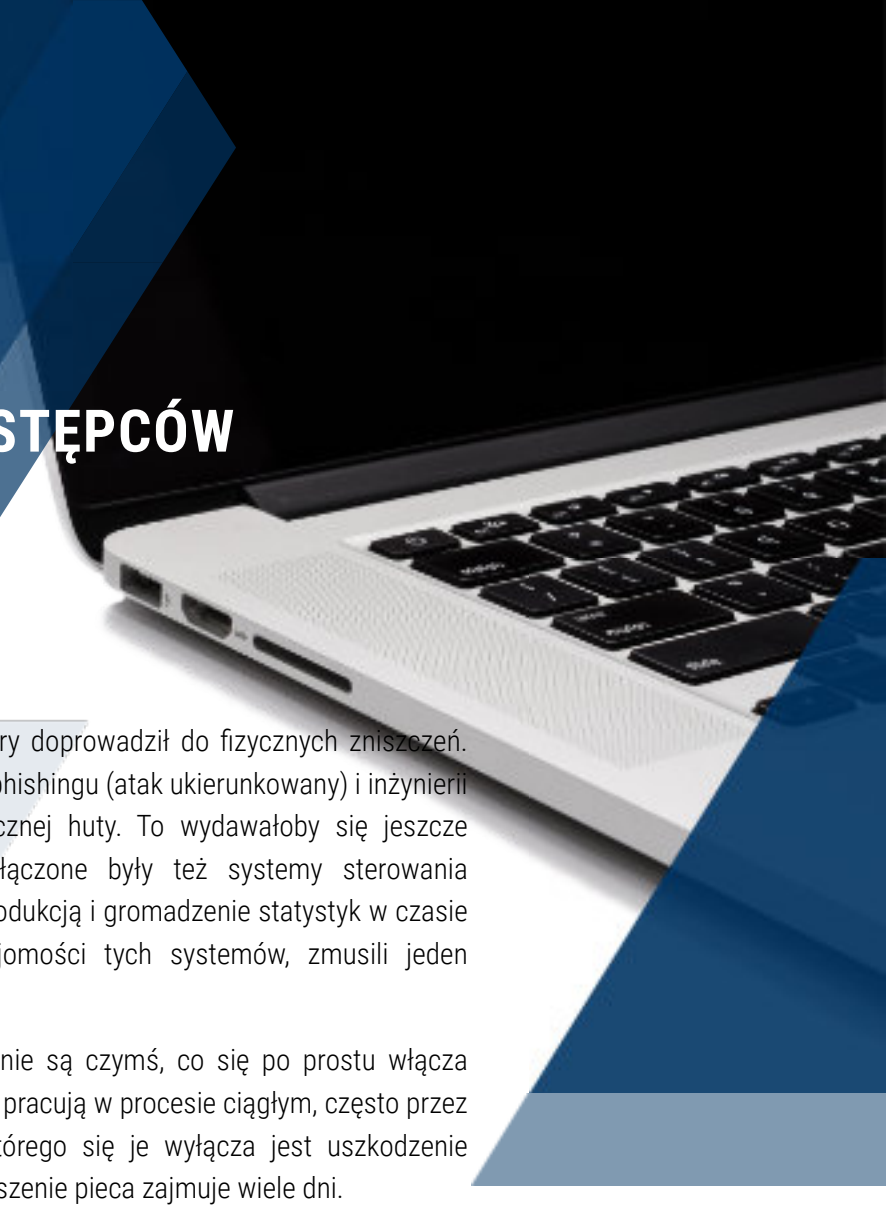
https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#28478e594f9a

4

Na skutek włamania do sieci Netii atakującym udało się wykraść dane osobowe klientów firmy. Dane zostały udostępnione w sieci. Wśród wykradzionych danych znajduje się między innymi historia zamówień składanych przez formularz WWW zawierająca pełne dane osobowe internautów, którzy chcieli zakupić usługi tej firmy.

https://zaufanatrzeciastrona.pl/post/uwaga-dane-klientow-netii-wykradzione-i-ujawnione-przez-wlamywaczy

PRZYKŁAD
DZIAŁANIA CYBERPRZESTĘPCÓW
a fizyczne zniszczenia



PRZYPADEK:

Niemiecka huta stali stała się ofiarą cyberataku, który doprowadził do fizycznych zniszczeń. Napastnicy wykorzystali wyrafinowane techniki spearphishingu (atak ukierunkowany) i inżynierii społecznej, by uzyskać dostęp do sieci informatycznej huty. To wydawałoby się jeszcze niegroźne, ale okazuje się, że do sieci tej podłączone były też systemy sterowania przemysłowego, tak by ułatwić zdalne zarządzanie produkcją i gromadzenie statystyk w czasie rzeczywistym. Hakerzy korzystając ze swojej znajomości tych systemów, zmusili jeden z wielkich pieców do niekontrolowanego wyłączenia.

Warto tu wyjaśnić, że wielkie piece w hutach stali nie są czymś, co się po prostu włącza i wyłącza. Te ogromne, około 40-metrowe konstrukcje pracują w procesie ciągłym, często przez wiele lat bez przerwy, a jedynym powodem dla którego się je wyłącza jest uszkodzenie ogniotrwałej izolacji. Nawet wówczas poprawne wygaszenie pieca zajmuje wiele dni.

Może się wydawać, że podobny scenariusz jest nieprawdopodobny w polskich realiach, niestety będzie to złudne wrażenie. Złośliwe oprogramowanie może zostać wprowadzone równie dobrze w wyniku ataku przygotowanego wyłącznie na daną spółkę, jak i w wyniku masowego ataku, który nie będzie skierowany na żadną konkretną ofiarę.

WNIOSKI:

Wystąpienie ataku tego rodzaju nie jest nowym zjawiskiem. Znane są przykłady podobnych ataków chociażby na Saudi Aramco. Najprościej mówiąc dzisiejsi cyberprzestępcy mogą przy pomocy zdalnego ataku wpływać na fizyczne funkcjonowanie elementów systemów IT a przez to przejąć kontrolę nad liniami produkcyjnymi czy konkretnymi urządzeniami. Prowadzić to może do kompletnego paraliżu poprawnego funkcjonowania całej spółki. Zwrócić uwagę należy, że większość podmiotów gospodarczych funkcjonuje na zasadzie systemu naczyń połączonych. Brak działania np. księgowości powoduje przestoje i wymierne straty. W tle skutków, które dotyczą nas bezpośrednio w wyniku ataku pozostaje zawsze aktualne ryzyko utraty reputacji czy zaufania naszych kontrahentów. Te, niestety nawet z czasem mogą okazać się nieodwracalne.

WIZUALIZACJA #1

W firmie zajmującej się produkcją płyt meblowych, której system pił sterowany jest komputerowo dochodzi do infekcji złośliwym oprogramowaniem. Zmienione zostają parametry szerokości cięcia czy kąt wycinania poszczególnych elementów. Pracownicy po jakimś czasie zauważają błędy w produkcjii wstrzymują linię produkcyjną.

SKUTKI

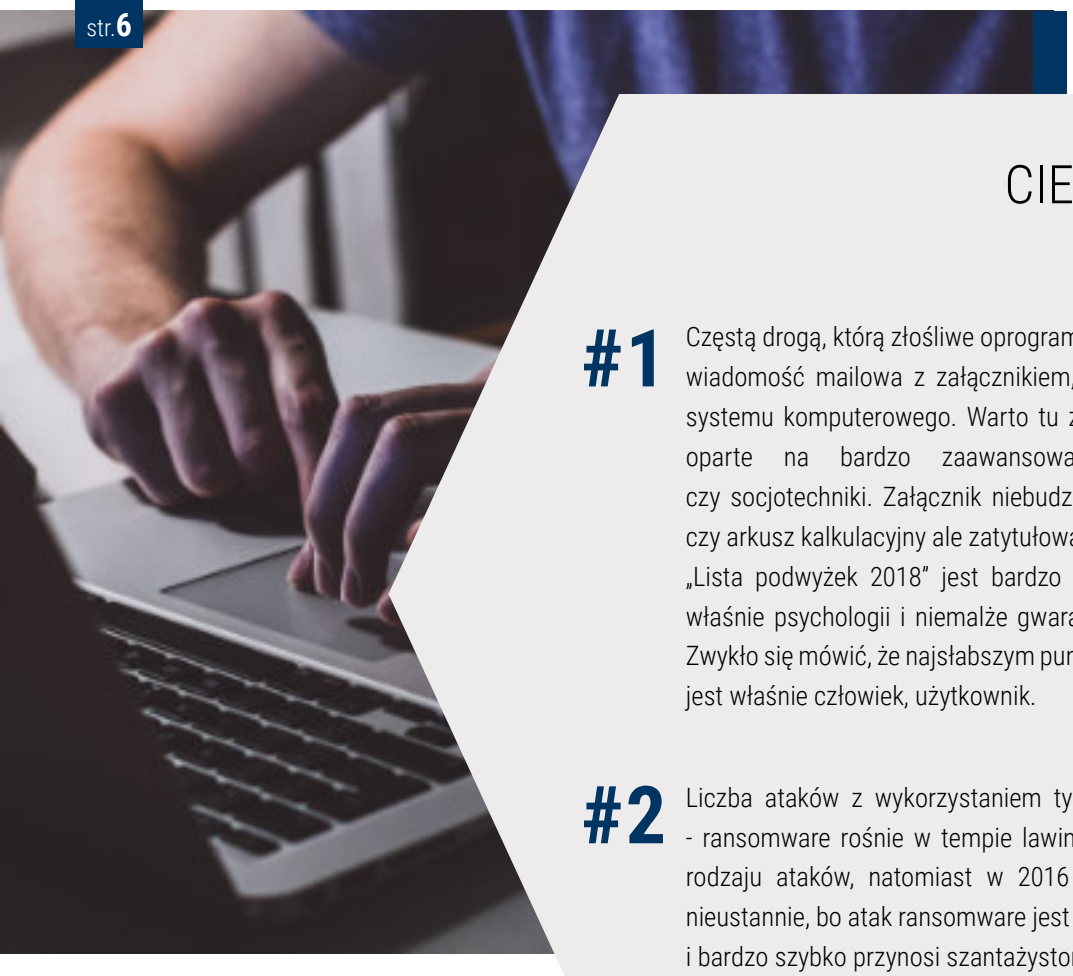
- konieczność zatrudnienia specjalistów, którzy zlokalizują źródło infekcji oraz przywrócą poprawne funkcjonowanie sysztemu produkcyjnego,
- strata finansowa wynikająca z opóźnień w produkcji,
- strata finansowa wynikająca z wyprodukowania towaru, który nie spełnia wymogów naszego kontrahenta.

WIZUALIZACJA #2

W spółdzielni mieszkaniowej pracownica sekretariatu otrzymała mail z adresu mailowego biuro@twojezloteraczki.pl zawierającego załącznik „Życzenia Wielkanocne 2018". Nie wzbudziło to jej podejrzeń, bowiem spółdzielnia podejmuje stałą współpracę z firmą „Twoje Złote Rączki" świadczącą usługi serwisowe wind i zsypów znajdujących się w zasobach spółdzielni. Mail jednak pochodzi z adresu gdzie zamiast aliasu.eu jaki ma zastosowanie w przypadku tej firmy, występuje alias.pl. Po otwarciu załącznika komputer został zainfekowany oprogramowaniem typu ransomware, wkrótce potem wszystkie komputery działające w spółdzielni. Autorzy ataku zaszyfrowali w ten sposób wszystkie komputery i żądają opłacenia okupu w wysokości 300$ za każdy kod odblokowujący stacje robocze.

SKUTKI

- konieczność poniesienia kosztów zatrudnienia informatyków, specjalizujących się w odzyskiwaniu danych, co niestety i tak wielokrotnie nie przynosi rezultatu,
- konieczność opłaty okupu, co jednak nie gwarantuje odblokowania stacji roboczych,
- na końcu jedyną możliwością może okazać się żmudny proces odtworzenia funkcjonalności systemu komputerowego poprzez ponowne skonfigurowanie wszystkich stacji roboczych, dane zaszyfrowane na dyskach mogą pozostać nieodzyskane.



CIEKAWOSTKI NA TEMAT
źródła zagrożenia

#1 Częstą drogą, którą złośliwe oprogramowanie dostaje się do naszego systemu jest wiadomość mailowa z załącznikiem, którego otwarcie powoduje zainfekowanie systemu komputerowego. Warto tu zwrócić uwagę iż ataki tego typu są często oparte na bardzo zaawansowanych rozwiązaniach psycho-manipulacji czy socjotechniki. Załącznik niebudzący podejrzeń, jak każdy inny plik tekstowy czy arkusz kalkulacyjny ale zatytułowany „Redukcja etatów – wiosna 2018" czy też „Lista podwyżek 2018" jest bardzo sprytnym rozwiązaniem z punktu widzenia właśnie psychologii i niemalże gwarantuje, że pracownik taki załącznik otworzy. Zwykło się mówić, że najsłabszym punktem systemu ochrony bezpieczeństwa sieci jest właśnie człowiek, użytkownik.

#2 Liczba ataków z wykorzystaniem tylko jednej z metod ataku cybernetycznego - ransomware rośnie w tempie lawinowym. W 2015 roku doszło do 4 mln tego rodzaju ataków, natomiast w 2016 już do 638 mln i liczba ta będzie rosła nieustannie, bo atak ransomware jest stosunkowo prosty do wykonania, skuteczny i bardzo szybko przynosi szantażystom profity. Szacuje się, że stosując wyłącznie tą metodę wymuszenia przestępcy osiągają kilka miliardów dolarów zysku w skali roku.

RODO
ROZPORZĄDZENIE O OCHRONIE DANYCH OSOBOWYCH

Dotychczasowe przepisy o ochronie danych osobowych i wydane rozporządzenia przewidywały, iż za niezgodne z prawem przetwarzanie danych kara nie mogła być wyższa niż 10 tys. zł w stosunku do osób fizycznych lub 50 tys. zł w stosunku do osób prawnych.

Przepisy obowiązujące od 25 maja 2018 roku, oznaczają już znacznie wyższe kary. Każda instytucja musi wdrożyć odpowiednie procedury bezpieczeństwa i zbudować system raportowania. Kary mogą sięgnąć **20 milionów euro** lub **4 proc. światowego obrotu firmy**. W nowej rzeczywistości prawnej nie ma już możliwości „zamiatania pod dywan" wycieków danych. RODO to m.in. obowiązek dla administratorów do zawiadamiania organu ochrony danych o naruszeniu przepisów w przypadku wykrycia naruszeń i ochrony danych osobowych w ciągu 72 godzin.

Zagrożenia cybernetyczne niestety zwiększają ryzyko wycieku danych i możliwość otrzymania wysokich kar. Kary to jednak nie jedyne zagrożenie, przed którymi stoi administrator danych. **Jedną z metod transferu ryzka jest ich ubezpieczenie.**

UBEZPIECZENIE
RYZYK CYBERNETYCZNYCH JAKO ROZWIĄZANIE PROBLEMU

Po ewentualnym ataku pokryje ono:

- koszt przywrócenia poprawnego działania systemu ponownej instalacji programów, konfiguracji, odtworzenia danych itp.,
- koszt okupu opłaconego w celu odszyfrowania danych,
- koszt zatrudnienia informatyków śledczych mających odkryć źródło i skalę ataku,
- utratę zysku w okresie przywracania do pełnej sprawności systemów spółki,
- koszt alternatywnych środków np. komunikacji z kontrahentami w okresie, gdy systemy są zablokowane,
- koszt odszkodowań, które przyjdzie zapłacić w związku z roszczeniem osoby, której dane przechowywaliśmy, a które zostały wykradzione,
- kwoty kar administracyjnych - w tym tych nakładanych na podstawie RODO,
- koszt skorzystania z usług agencji public relations, kiedy dojdzie do np. kradzieży danych w celu ratowania reputacji spółki jak i osób fizycznych sprawujących funkcje kierownicze.

Nie ma w dzisiejszej rzeczywistości firm bezpiecznych.
Nie jest tajemnicą, że w sieci można zakupić szkodliwe oprogramowanie, czy prosty atak hakerski już za kilkadziesiąt dolarów. Skutki takiego ataku będą liczone nawet w milionach złotych… zatem, czy możemy w 100% stwierdzić, że nie jesteśmy zagrożeni ponieważ:

- nasz system IT jest niezawodny,
- nasze systemy zabezpieczeń obsługują podmioty zewnętrzne,
- nic nam nie grozi, bo firma jest mała,
- nasza infrastruktura jest niezawodna,
- nie działamy w atrakcyjnej dla przestępców branży?

Ubezpieczenie CYBER pokrywa koszty, które ponosimy, kiedy do ataku już dojdzie w celu zmniejszenia jego skutków, czy też przywrócenia normalnego działania systemu. Gwarantuje bezpieczeństwo finansowe na wypadek kar administracyjnych, czy odszkodowań dla osób poszkodowanych w wyniku wycieku danych.

MAJKOWSKI BROKERS
GRUPA FST
20 LECIE 1998-2018

www.majkowski.pl

SIEDZIBA
ul. Korczaka 24/4
83-200 Starogard Gdański
sekretariat@majkowski.pl
tel. +48 58 563 36 00
fax +48 58 563 36 11

ODDZIAŁ
ul. Zgoda 13/2
81-361 Gdynia
gdynia.biuro@majkowski.pl
tel. +48 58 661 45 67
fax +48 58 620 88 52