Ochrona informacji w kancelarii adwokackiej

Jakub Bojanowski

19 listopada 2024

Trochę o mnie

- Jestem informatykiem, ale przed wszystkim doradcą i menedżerem z ponad 25 letnim doświadczeniem. Przez wiele lat byłem wspólnikiem w międzynarodowej firmie doradczej i szefem zespołu Zarządzania Ryzykiem w Polsce i Europie Centralnej.
- Problematyką cyberbezpieczeństwa zajmuję się od 1999 roku kiedy to współpracowałem z jednym z największych banków w Polsce przy opracowaniu polityki bezpieczeństwa informacji. W 2000 roku wykonywałem tzw. „testy penetracyjne" poprzedzające uruchomienie jednego z pierwszych systemów bankowości online w Polsce.
- Obecnie koncentruję się na roli nauczyciela akademickiego w Akademii Leona Koźmińskiego i Polsko - Japońskiej Akademii Technik Komputerowych, oraz współpracuję przy projektach edukacyjnych organizowanych różne instytucje biznesowe
- Jestem autorem książki „**Zdążyć przed hakerem**", przybliżającej tematykę cyberbezpieczeństwa menedżerom nie dysponującym specjalistyczną wiedzą techniczną.

Tematyka spotkania

- Krajobraz cyberzagrożeń – w jaki sposób działają hakerzy i cyberprzestępcy.
- Profil cyberryzyka – dlaczego kancelaria prawna jest atrakcyjną ofiarą cyberprzestępców.
- Przechowywanie danych: komputery firmowe, osobiste i chmura obliczeniowa.
- Korzystanie z poczty: ochrona tożsamości, szyfrowanie wiadomości, podpis elektroniczny.
- Komputer poza siedzibą kancelarii: ochrona w sieci klienta, korzystanie z WiFi i VPN.

Cyber mity i cyber rzeczywistość

gov.pl | Serwis Rzeczypospolitej Polskiej

Strona główna
Rada Ministrów
Kancelaria Premiera
Ministerstwa
Urzędy, instytucje i placówki RP

Usługi dla obywatela
Usługi dla przedsiębiorcy
Usługi dla urzędnika
Usługi dla rolnika

Profil zaufany
Baza wiedzy
Serwis Służby Cywilnej
Сайт для громадян України –Serwis dla obywateli Ukrainy

Rosyjski wywiad wykorzystuje CVE JetBrains w globalnej kampanii

13.12.2023

Rosyjska Służba Wywiadu Zagranicznego (SVR) wykorzystuje podatność CVE-2023-42793 do szeroko zakrojonych działań, skierowanych przeciwko serwerom oprogramowania JetBrains TeamCity.

CERT.PL NASK | National Cyber Security Centre

Federalne Biuro Śledcze (FBI), Amerykańska Agencja Bezpieczeństwa Cybernetycznego i Infrastruktury (CISA), Narodowa Agencja Bezpieczeństwa (NSA), Brytyjskie Narodowe Centrum Bezpieczeństwa Cybernetycznego (UK NCSC), Polska Służba Kontrwywiadu Wojskowego (SKW) oraz CERT Polska (CERT.PL) wykryły, że Rosyjska Służba Wywiadu Zagranicznego (SVR) wykorzystuje podatność CVE-2023-42793 do szeroko zakrojonych działań, skierowanych przeciwko serwerom

SZKOLENIA KONTAKT REKLAMA WIDEO SECURITY AWARENESS

Zaufana Trzecia Strona

Wyniki badań medycznych kilkudziesięciu tysięcy Polek i Polaków ujawnione przez włamywaczy

Adam Haertle dodał 27 listopada 2023 o 00:08 w kategorii Info, Włamania z tagami: ALAB • dane medyczne • dane osobowe • ransomware • wyciek

Do internetu trafiły wyniki badań medycznych wykonanych przez ostatnie kilka lat w jednej z największych ogólnopolskich sieci laboratoriów medycznych, firmy ALAB. Wyciek jest skutkiem ataku grupy ransomware, a dane to podobno tylko próbka.

To jeden z tych artykułów, których wolelibyśmy nigdy nie napisać. Niestety skutki tego ataku ransomware odczuje co najmniej kilkadziesiąt tysięcy Polek i Polaków, którzy od roku 2017 do 2023 wykonywali badania medyczne w sieci ALAB laboratoria. Szerzej nieznana grupa ransomware RA World opublikowała na swoim blogu nie tylko informację o skutecznym włamaniu do firmy ALAB, ale także próbkę wykradzionych danych – a niej między innymi wyniki ponad 50 tysięcy badań medycznych.

/ Cyfrowa / IT

Rosyjski atak na Pocztę i Modlin. Za Ukrainę

Prokremlowskie grupy cybernetyczne uderzyły w strategiczne cele transportu lotniczego i kolejowego w naszym kraju.

Publikacja: 06.11.2023 11:28

Nasza percepcja cyberzagrożeń

- Czy moja kancelaria adwokacja jest narażona na cyberataki.
- Jakiego typu atak stanowi dla mnie „czarny scenariusz” czyli może realnie zagrozić mojej kancelarii:
  - wykradzenia danych „wewnętrznych” dotyczących działalności kancelarii (obroty, płace, koszty administracyjne);
  - kradzież środków z rachunku bankowego;
  - unieruchomienie systemów komputerowych (serwera, albo poszczególnych komputerów);
  - utrata danych dotyczących klientów (naruszenie tajemnicy zawodowej);
  - podmiana strony www kancelarii;
  - kampania „czarnego PR” w mediach społecznościowych;
  - wyciek danych osobowych i kara z UODO.

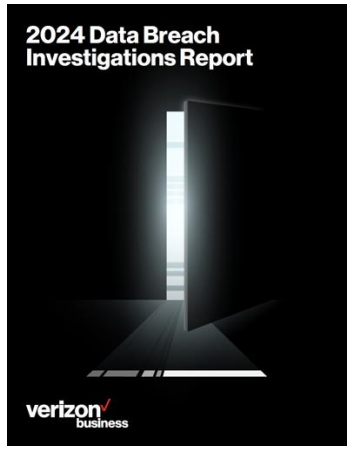
- Jakiego typu atak jest najbardziej prawdopodobny:
  - czy kancelaria jest narażona na ataki „rosyjskich hakerów” ?
  - jak reagujemy na kolejne doniesienia medialne na temat kolejnych cyberincydentów ?

Data Breach Investigations Report – przykład profesjonalnej analizy cyberzagrożeń

- Coroczna publikacja analizująca incydenty z zakresu cyberbezpieczeństwa:
  - ukazuje się od 2008 roku;
  - oparty na jednolitej taksonomii co pozwala śledzić trendy w cyberbezpieczeństwie;
  - analizy pod kątem charakteru, metod ataku, sprawców i skutków zdarzenia;
  - dane są analizowane w ujęciu globalnym, podział i analizy według poszczególnych branż gospodarki i regionów;
  - zawiera kalendarium kluczowych globalnych wydarzeń z zakresu cyber.

- Baza stanowiąca podstawę raportów DBIR obejmuje ponad milion incydentów:
  - w raporcie z 2024 po raz pierwszy przeanalizowano ponad 10 000 Incydentów.

- Autorem jest Verizon – wiodący dostawca usług telekomunikacyjnych:
  - raport jest dostępny publicznie, z prawem do cytowania.



Źródło: https://www.verizon.com/business/resources/reports/dbir/

Aktorzy - kim są cyberprzestępcy

- Od wielu lat motywacja finansowa przeważa nad innymi celami cyberataków.
- Głównym sprawcą ataków jest przestępczość zorganizowana.
  - wbrew oczekiwaniom, wojna w Ukrainie nie zmieniła znacząco tej sytuacji.
  - cyberataki związane z „wojną hybrydową” są szeroko nagłośnione w mediach, ale nie wpływają istotnie na obserwowane trendy;
  - ataki sponsorowane przez agendy rządowe dotyczą tylko wybranych sektorów gospodarki – mają mniejszy wpływ na „typowe” firmy i instytucje.
- Skala „tradycyjnej” cyberprzestępczości jest zbyt duża, aby inne cele ataku mogły mieć istotne znaczenie dla statystyk.

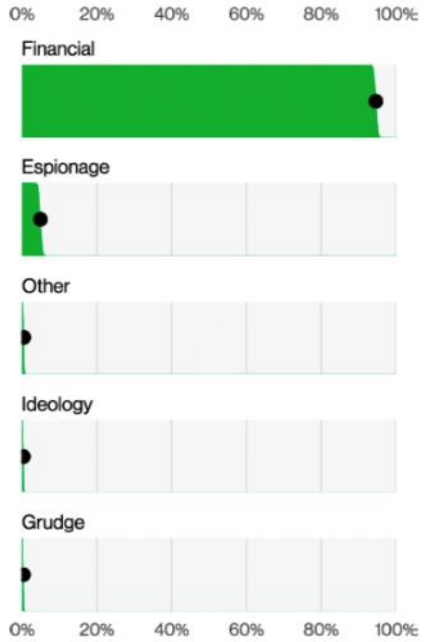


Figure 12. Threat actor Motives in breaches (n=2,328)

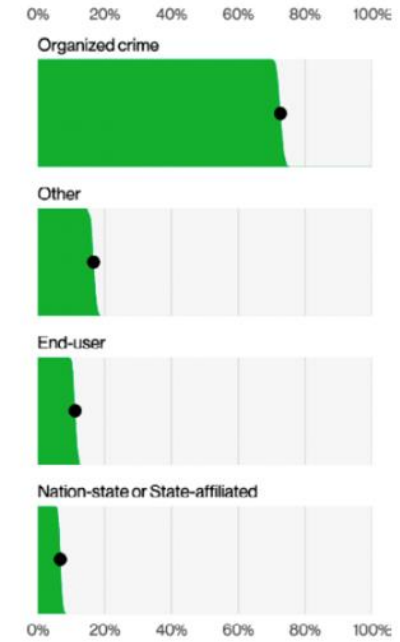


Figure 13. Threat actor Varieties in breaches (n=2,489)

Źródło: https://www.verizon.com/business/resources/reports/dbir/

„Wektory ataku” współczesnych cyberprzestępstw

- Ransomware
  - wymuszanie okupu poprzez zaszyfrowanie danych i unieruchomienie komputerów;
  - coraz częstsze próby okupu w zamian za nieujawnienie danych;
  - kilka poważnych, potwierdzonych incydentów wypłaconych okupów przekraczających 1M USD.
- Business Email Compromise / Pretexting
  - utrata środków finansowych w reakcji na sfałszowany mail (dyspozycja płatności lub zmiana numeru konta);
  - według FBI (dane sprzed kilku lat) - skala strat finansowych rzędu 13 miliardów USD rocznie;
  - co najmniej jeden znany przypadek w udziałem polskiej spółki Skarbu Państwa.
- Phishing
  - wysyłanie złośliwego oprogramowania w mailu (80%) lub wiadomości SMS;
  - ma formę linku często schowanego za załącznikiem do dokumentu (75%);
  - najbardziej znana forma ataku, ale wyjątkowo skuteczna.
- Computer Data Breach
  - bezpośrednie straty w wyniku wycieku informacji;
  - nagłaśniane są głównie przypadki związane z wyciekiem danych osobowych.

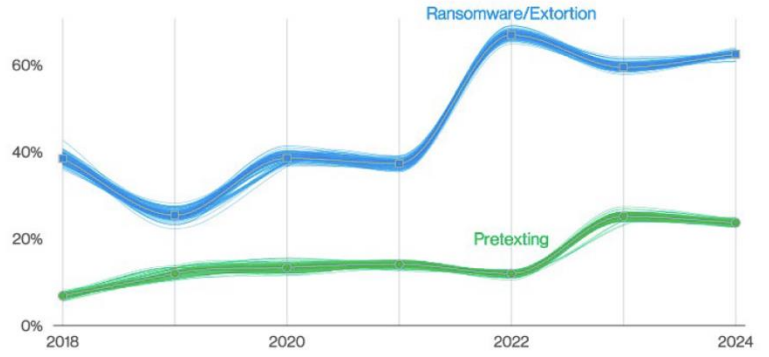


Figure 18. Select action varieties in Financial motive over time

Źródło: https://www.verizon.com/business/resources/reports/dbir/

Ransomware

- Atak polega na wymuszaniu okupu przez zaszyfrowanie danych na komputerach.
- Często jego podstawą jest groźba ujawniania danych (pozyskanych w wyniku włamania).
- Ofiary (firmy i osoby prywatne) są zaskakująco podatne na tego typu groźby:
  - znane są incydenty gdzie firmy zapłaciły okupy przekraczające miliony USD.

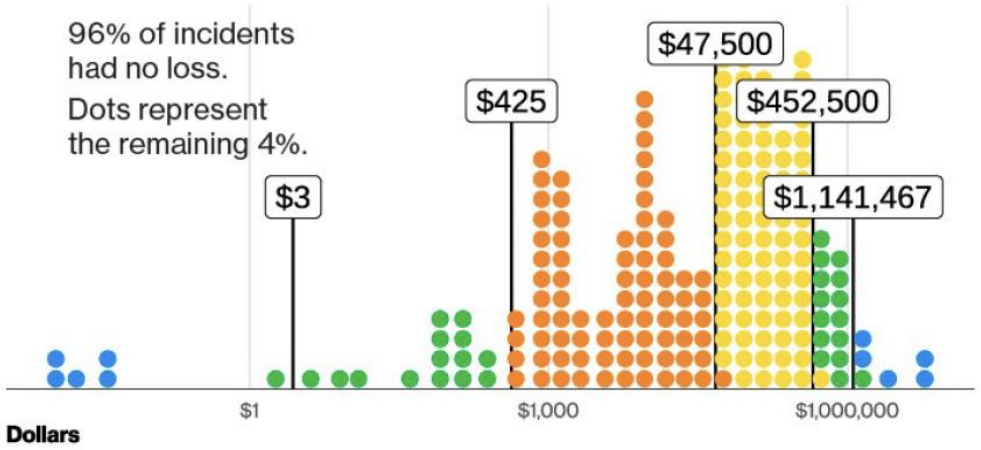


Figure 30. 95% and 80% confidence intervals of adjusted incident cost for Ransomware

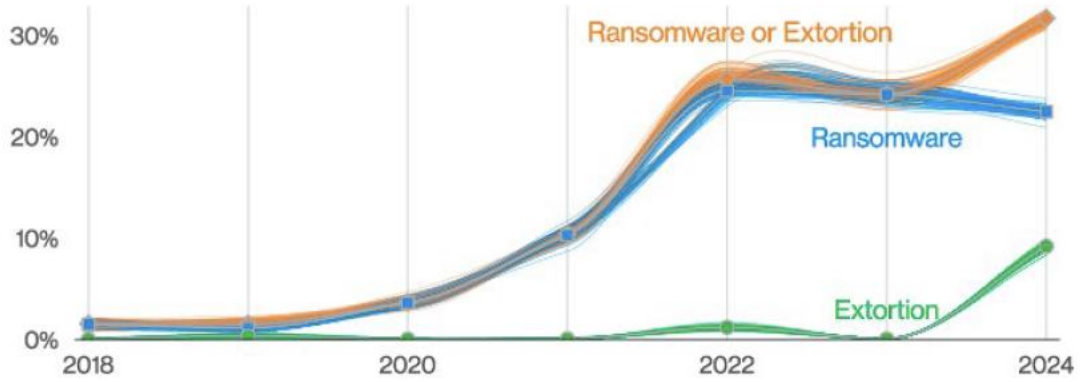
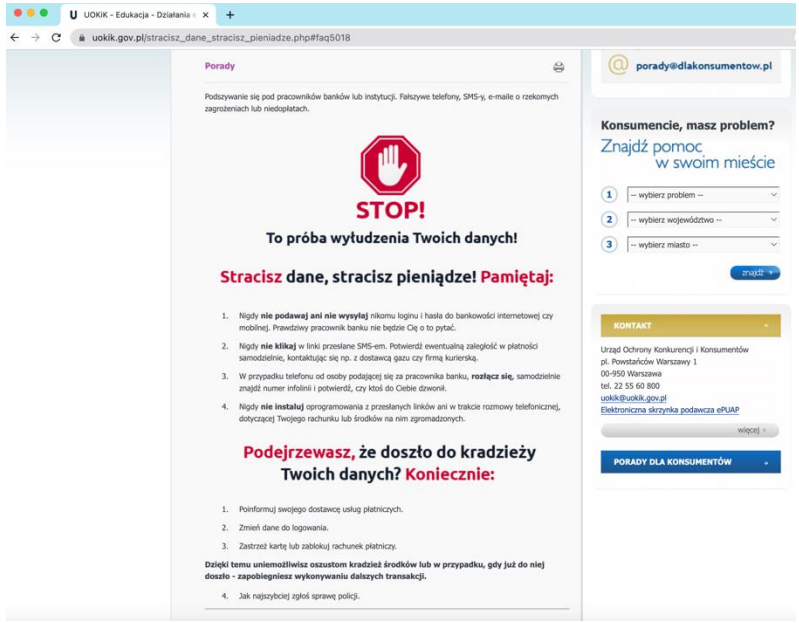


Figure 33. Ransomware and Extortion breaches over time

Źródło: https://www.verizon.com/business/resources/reports/dbir/

Podatność na „inżynierię społeczną”

- Od czasu COVID-19 obserwujemy wzrost liczby PROSTYCH ataków opartych na wyłudzeniu informacji (dostępu do konta bankowego lub komputera), a nie na przełamywaniu zabezpieczeń technicznych.
  - źródłem tego zjawiska jest „nowa” grupa internautów, którzy zaczęli korzystać z komputerów dopiero w trakcie pandemii;
  - od pandemii wiele osób korzysta z komputerów „z konieczności”. Są one gorzej wyedukowane w zakresie cyberbezpieczeństwa.



Business Email Compromise

- Najnowsze statystyki pokazują rosnącą popularność prostych ataków (tzw. pretexting) – np. polegających na wysłaniu pocztą informacji o zmianie numeru rachunku bankowego:
  - ataki nie wymagają żadnych umiejętności technicznych i ich popularność rośnie (zgodnie z danymi Verizon przekroczyła phishing);
  - ataki są statystycznie mniej skuteczne od phishingu, ale i tak zapewniają cyberprzestępcom wystarczającą skalę działalności.

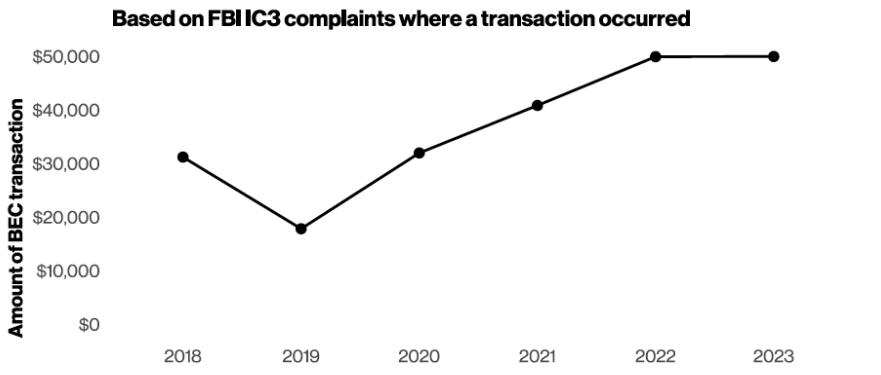


Figure 36. Median transaction size for BECs

Figure 34. Top Action varieties in Social Engineering incidents (n=3,647)

Źródło: https://www.verizon.com/business/resources/reports/dbir/

Menedżer (prawnik) jako źródło zagrożenia

- Badania naukowy pokazują, że kadra menedżerska jest grupą zawodową w największym stopniu dotkniętą ”wykluczeniem cyfrowym”. Wiedza na temat technologii u „typowego” menedżera jest znacznie niższa niż u typowego pracownika.

- Komputery (poczta) menedżerów stanowią atrakcyjne trofeum dla hakerów.

- „Prezesi” są bardziej podatni na szantaż:
  - „mają więcej do stracenia”;
  - mają możliwości działania niedostępne dla szeregowych pracowników.

- W dużej korporacji pracownik, którego komputer zaatakowano musi iść do szefa, bo sam nie uruchomi środków na zapłacenie okupu. W niewielkiej firmie (kancelarii) ofiara szantażu jest jednocześnie dysponentem środków.

Skrzynki poczty elektronicznej i zabezpieczajace je hasła

- Rola w organizacji:
  - teoretycznie: narzędzie do osobistej komunikacji pomiędzy osobami;
  - w praktyce: repozytorium informacji biznesowych;
- Typowe cele ataku hakera:
  - podsłuch lub kradzież informacji;
  - fałszowanie poczty;
  - przejęcie kontroli nad skrzynką pocztową użytkownika.

- Przejęcie poczty oznacza możliwość wykorzystania jej do przejęcia kont na pozostałych usługach sieciowych (zmianę „zapomnianego” hasła realizujemy za pomocą poczty).

- Obecnie poczta elektroniczna stanowi główne narzędzie i cel cyberataków jednocześnie najczęściej (prywatna) poczta jest najgorzej zabezpieczonym zasobem IT.
- W niewielkiej kancelarii granica między prywatną i służbową pocztą jest bardzo „płynna”.

Które z poniższych haseł możemy uważać za najlepsze:

HASŁO

Tb,ontb?

uszewczykaleZAjakdiabeLmLodzieNcy

,AiGyrcsJSPZGJ1)O;U,

12345

Papuga2024

W6a-o!jw!Pkk”zb!

uprzasniczkisiedzajakanioldzieweczki

L,om!tjjz

Dobra praktyka postępowania z hasłami

- Hasła powinny być trudne dla odgadnięcia.
- Haseł nie zapisujemy w formie, która umożliwia ich łatwe odtworzenie.
- Hasła powinny być łatwe do zapamiętania, aby nie było potrzeby ich zapisywania.
- Nie powinniśmy wykorzystywać tych samych haseł w różnych systemach, szczególnie jeżeli posługujemy się w nich tym samym identyfikatorem użytkownika.
- Hasło traktujemy jako zasób prywatny i w żadnej formie nie udostępniamy go innej osobie.
- Wpisując hasło do systemu, upewniamy się, że nie jesteśmy obserwowani.
- Pomimo powyższych zasad zakładamy, że nasze hasło może zostać ujawnione. Okresowo zmieniamy je (zazwyczaj co 30 lub 90 dni).

Przykład dobrego hasła – metoda 1

- W6a-o!jw!Pkk”zb!
- Wykorzystujemy pierwsze litery wiersza, cytatu, lub motta
- Zalety:
  - wielkie i małe litery, znaki specjalne;
  - solidna długość: 16 znaków;
  - łatwe do zapamiętania:
    - W6a-o!jw!Pkk”zb! - W szóstym armata, o! jaka wielka! Pod każdym kołem żelazna belka!
- Wady:
  - wykrzyknik ! znajduje się na klawiszu z nr 1 i jest najczęściej stosowanym przez użytkowników znakiem specjalnym;
  - kolejnym najczęściej stosowanym jest znak @ – klawisz nr 2;
  - użytkownicy zmuszani do użycia znaku specjalnego najczęściej umieszczają go na końcu hasła.

Przykład dobrego hasła – metoda 2

- SpadlpiesekPODogrodzenieIwyje
- Modyfikujemy (w nieoczywisty sposób) słowa w znanym fragmencie tekstu zastępując je podobnymi
- Łączymy co najmniej 5—6 słów
- Zalety:
  - dowolna długość hasła : 28 znaków;
  - łatwe do zapamiętania:
  - „Wlazł kotek na płotek i mruga”
- Wady:
  - brak znaków specjalnych (ale zrekompensowany długością hasła)
  - w tym przypadku – dość oczywista zamiana słów

Ćwiczenie: hasła - rozwiązanie

12345	HASŁO
Papuga2024	
Tb,ontb?	L,om!tjjz
uprzasniczkisiedzajakanioldzieweczki	,AiGyrcsJSPZGJ1)O;U,
W6a-o!jw!Pkk”zb!	**uszewczykaleZAjakdiabeLmLodzieNcy**

Silne uwierzytelnienie

Silne uwierzytelnienie (ang. *strong authentication*), albo uwierzytelnienie dwuskładnikowe (ang. *two factor authentication*, *2FA*) oparte na zastosowaniu co najmniej dwóch niezależnych elementów należących do dwóch z trzech kategorii:

- wiedza (ang. *something you know*): hasło, PIN, wiedza z dzieciństwa
- posiadanie (ang. *something you have*): telefon, token, karta kredytowa
- cecha osobowa (ang. *something you are*): odcisk palca, twarz

Silne uwierzytelnienie poważnie komplikuje życie hakerom:

- wymóg prawny przy dokonywaniu płatności internetowych
- dobra praktyka przy dostępie do poczty elektronicznej (także prywatnej)

Jednym z bardziej skutecznych sposobów przełamania 2FA jest przejęcie telefonu komórkowego, który jest najczęstszym elementem „posiadania” przy silnym uwierzytelnieniu

- uważajmy na telefony !!!

Dlatego przy (kwalifikowanym) podpisie elektronicznym klucz jest umieszczony na dodatkowym urządzeniu.

Menedżer haseł i klucze sprzetowe

Typowy internauta korzysta z ponad 100 usług zabezpieczonych hasłem. Oznacza to, że:

- stosujemy to samo hasło do różnych systemów;
- zapisujemy hasła w niedostatecznie zabezpieczony sposób;
- nadużywamy możliwości resetowania hasła za pomocą poczty elektronicznej.

Standardem powinno być korzystanie z menedżera haseł czyli usługi zapisującej hasła w bezpiecznej formie i podpowiadającej je przy użyciu. Menedżer haseł może być:

- element systemu operacyjnego (Windows, macOS, iOS);
- element przeglądarki internetowej (Chrome);
- zewnętrzna dedykowana aplikacja (1password).

Ostatnio popularność zyskują klucze sprzętowe (U2F, youbikey) łączące funkcję menedżera haseł i czytnikiem biometrycznym:

- wykorzystanie kluczy jest dobrym pomysłem, ale użytkownicy muszą zadbać o ochronę tych urządzeń, a „w dużej korporacji ktoś na pewno taki klucz zgubi”;
- w „korporacji” pojawia się problem formalny czy taki klucz sprzętowy jest zasobem służbowym czy prywatnym;
- w „małej” kancelarii to może być dobre rozwiązanie.

Podsłuch i fałszowanie poczty elektronicznej

- Wszystkie informacje wysyłane pomiędzy komputerami podłączonymi do Internetu (także pocztą) są przesyłane przez punkty pośredniczące węzły sieci (tak zwane „routery”).
  - Osoby kontrolujące komputery pośredniczące w wymianie informacji w Internecie mają możliwość zapoznania się z przesyłaną informacją podobnie jak dawniej możliwe było podsłuchiwanie rozmów przez osoby obsługujące centrale telefoniczne.
- Korzystając z poczty elektronicznej musimy mieć świadomość tego ograniczenia.

- O ile nie stosujemy dodatkowego systemu szyfrowania poczty musimy założyć, że:
  - poczta elektroniczna nie zapewnia poufności przesyłanych nią informacji;
  - każda wiadomość wysłana pocztą elektroniczną może być przeczytana przez osoby postronne.
- Analogią do komunikacji pocztą elektroniczną jest wymiana informacji na pocztówkach

- Podobnie (choć nieco trudniejsze technicznie) możliwe jest sfałszowanie poczty elektronicznej, czyli wysłanie przesyłki z innego adresu niż rzeczywisty adres nadawcy. Z funkcjonalności tej cyberprzestępcy korzystają przy wysyłaniu przesyłek *phishingowych*.

Szyfrowanie i podpisywanie poczty

Metoda wysyłki informacji	Ocena rozwiązania
wysłanie informacji niezaszyfrowaną pocztą	• rozwiązanie nie spełnia jakichkolwiek standardów bezpieczeństwa informacji • musimy założyć, że wiadomość jest dostępna dla osób postronnych
zablokowanie załącznika (np. PDF) daną znaną odbiorcy (PESEL, REGON)	• często stosowane w praktyce (także w branży bankowej i ubezpieczeniowej) • chroni przesyłane informacje przed przypadkowym dostępem • nie zapewnia w pełni poufności informacji, gdyż dane wykorzystywane do zablokowania dokumentu są powszechnie znane • zaszyfrowanie załącznika chroni sam załącznik, a nie treść w całej przesyłki mailowej
zablokowanie (lub zzipowanie) załącznika uzgodnionym hasłem	• metoda często stosowana w praktyce w rozwiązaniach biurowych • zapewnia podstawowy poziom bezpieczeństwa pod warunkiem, że hasło jest odpowiednio silne (podobnie jak hasła stosowane do logowania się do systemu) • hasło musimy wymienić inną metodą niż poczta elektroniczna • zablokowane pliki w niektórych przypadkach mogą być zatrzymane przez systemy antywirusowe
szyfrowania poczty oparte na infrastrukturze klucza publicznego (podobnie jak kwalifikowany podpis elektroniczny)	• wymaga wcześniejszego uzgodnienia rozwiązania pomiędzy oboma stronami • jest stosunkowo trudne w instalacji (może wymagać pomocy technicznej) • po włączeniu: szyfruje (i podpisuje) całość komunikacji pomiędzy konkretnymi osobami

Jakie inne zasoby interesują cyberprzestępców – atak na firmę

- Sieć, urządzenia sieciowe:

  typowe cele hakera: przejęcie kontroli nad urządzeniem sieciowym; dołączenie dodatkowego urządzenia do sieci (np. w celu podsłuchu); atak typu DoS (odmowa dostępu).

- Usługi sieciowe, serwery aplikacyjne:

  typowe cele hakera: atak na serwer (przejęcie kontroli nad serwerem); atak na usługę (aplikację) i nieautoryzowane skorzystanie z usługi; zakłócenie dostępności usługi.

- Serwery w sieci wewnętrznej:

  typowe cele hakera: przejęcie kontroli nad serwerem; dostęp do danych; przejęcie identyfikatorów (loginów) i haseł użytkowników.

- Bazy danych, repozytoria danych:

  typowe cele hakera: wykradzenie informacji; nieuprawniona modyfikacja informacji; „skasowanie bazy”.

- Systemy przemysłowe:

  typowe cele hakera: przejęcie kontroli nad urządzeniem; zakłócenie pracy urządzeń sterowanych danym systemem (zatrzymanie linii produkcyjnej).

Jakie zasoby interesują cyberprzestępców – atak na użytkownika

- Komputery osobiste, urządzenia mobilne, przenośne nośniki danych:

  kradzież samego urządzenia;

  dostęp do danych zapisanych na urządzeniu;

  przejęcie kontroli nad urządzeniem jako narzędzia do dalszego ataku;

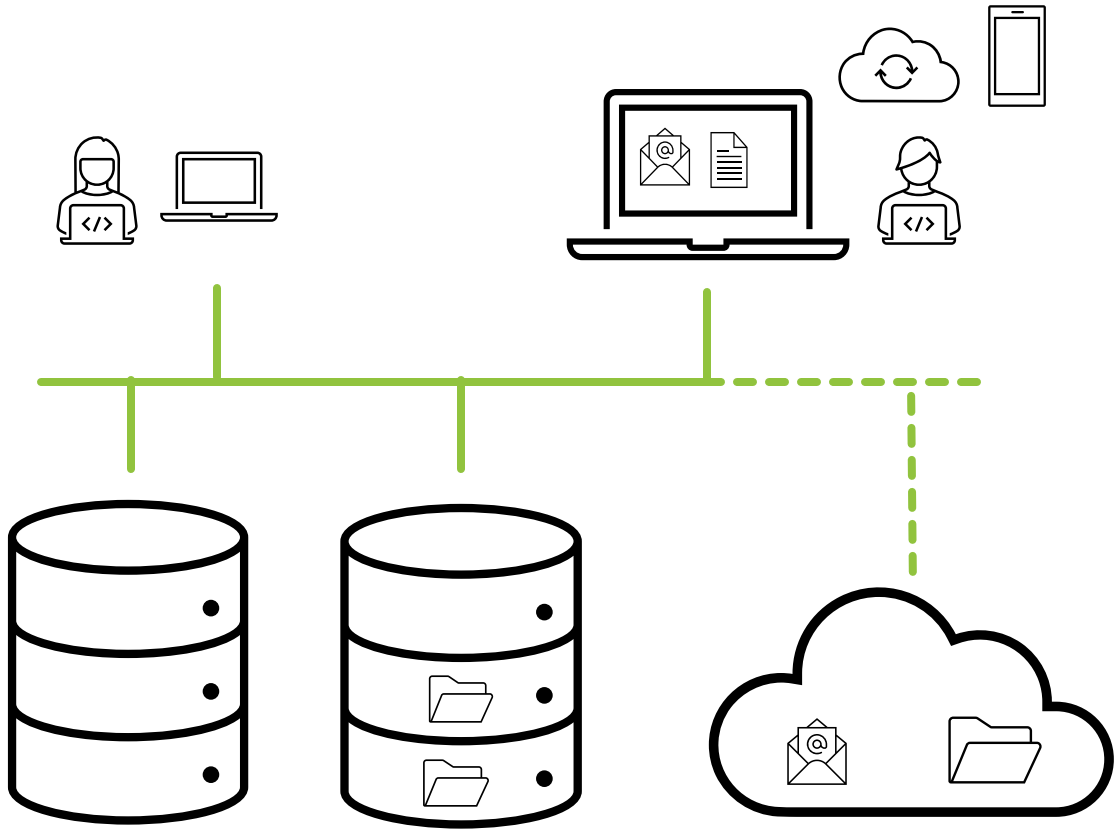
  ataki ransomware.

- Zasoby w chmurze obliczeniowej (infrastruktura, aplikacje, oprogramowanie):

  zasoby sieciowe (zewnętrzne) pełniące rolę serwerów, usług i aplikacji wewnętrznych

  UWAGA: Microsoft 365, w tym systemy biurowe: Word, Excel itp. to obecnie także chmura

Prawnik w sieci - korporacja



Komputer (telefon, tablet) prawnika:

- skrzynka poczty;
- system plików, dokumenty:
  - wieloletni „know-how”;
- zasoby w chmurze (użytkownika).

Dostęp do zasobów (serwerów) firmowych:

- wrażliwe katalogi (pliki);
- dokumenty dotyczące wrażliwych operacji.

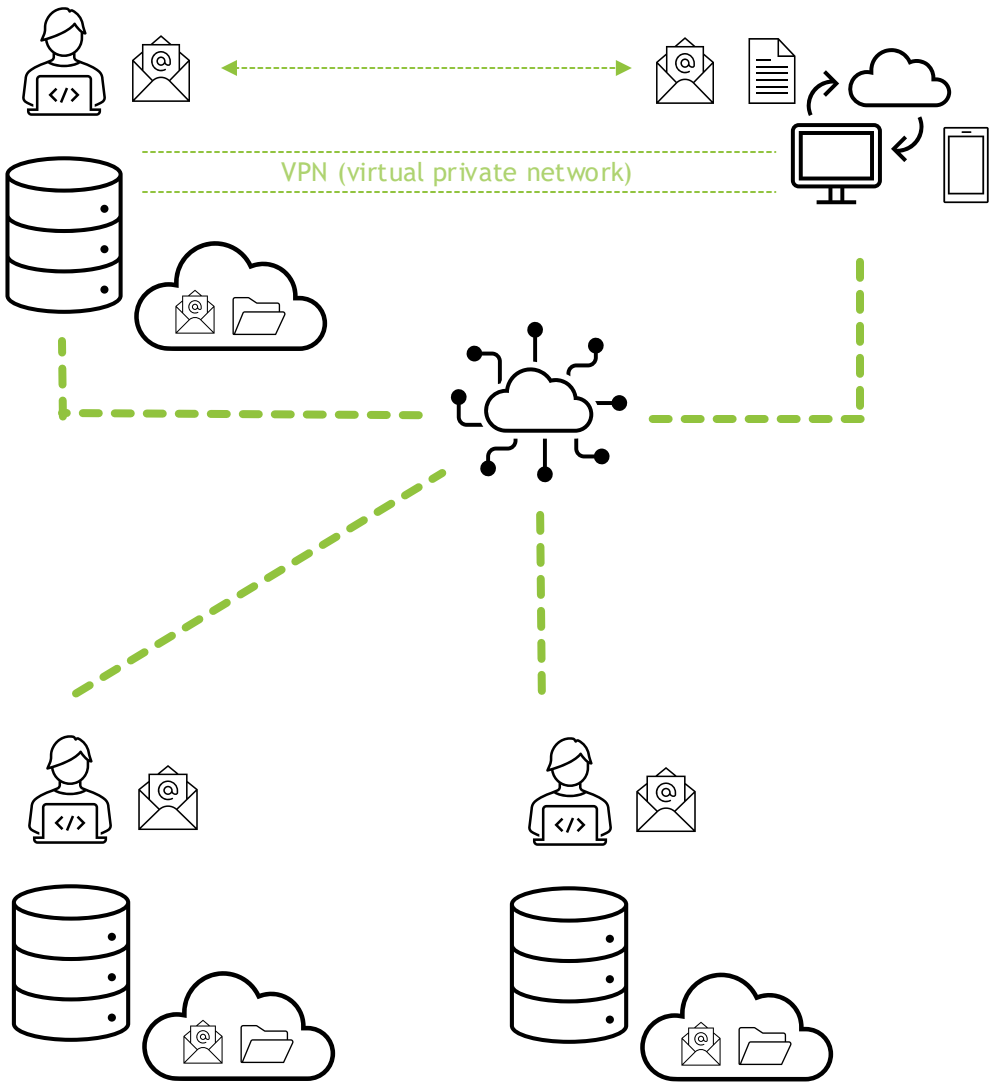
Firmowa chmura obliczeniowa:

- skrzynka poczty elektronicznej;
- dokumenty (Microsoft 365).

Chmury specjalne:

- e-room (przy transakcji M&A).

Prawnik w sieci – kancelaria zewnętrzna



Większość ryzyk IT pozostaje bez zmian, ale:

- więcej zasobów w chmurze obliczeniowej;
- gorszy know-how w zarządzaniu bezpieczeństwem;
- brak granicy między zasobami prywatnymi i służbowymi.

Wymiana informacji z klientem przez sieć (publiczną):

- rośnie rola poczty elektronicznej;
- konieczność szyfrowania informacji.

Dostęp zdalny do sieci klienta przez VPN:

- stanowimy zagrożenie dla klienta;
- jakie dane możemy kopiować miedzy siecią klienta i kancelarią;
- na ile obie strony rozumieją ryzyko prawne z tym związane

Komputer prawnika „łączy” sieci klientów:

- zaawansowana konfiguracja techniczna;
- bardzo zaawansowane know-how.

Prawnik w sieci – przedsiębiorca (mała kancelaria)

Typowa kancelaria prawna jest szczególnie podatna na zagrożenia typowe dla niewielkich firm

Business Email Compromise:

- w małej firmie trudniej o podział obowiązków w zakresie obsługi finansów

Phishing:

- nasze zabezpieczenia techniczne są zazwyczaj mniej zaawansowane niż w korporacjach;
- szkolenia z cyberbezpieczeństwa są nie tylko dla „pracowników – nie zapominajmy o sobie.

Ransomware:

- jesteśmy bardziej podatni na szantaż, bo ze względu na zaufanie klientów i przetwarzane dane mamy DUŻO do stracenia;
- łatwiej nam podjąć decyzję o wypłacie okupu - nie musimy trzymać się procedur.

Mini podsumowanie: zagadnienia „wysokiego ryzyka”

Zawartość komputera:

- Czy na pewno wszystkie informacje musimy przechowywać na swoim komputerze osobistym?
- Czy rozumiemy wagę informacji przechowywanych w naszej skrzynce pocztowej?

Zawartość urządzeń mobilnych:

- Czy jesteśmy przygotowani na utratę (kradzież) naszego urządzenia mobilnego?

Przechowywanie wrażliwych informacji:

- Czy polityka „czystego biurka” przekłada się na naszą codzienną praktykę korzystania z technologii?
- W ramach korzystania z technologii - jaki jest elektroniczny odpowiednik kasy pancernej?

Wymiana danych z klientami – SZYFROWANIE:

- Czy rozumiemy zagrożenia związane z wymianą informacji za pośrednictwem sieci?
- Czy na pewno konsekwentnie stosujemy adekwatne środki ochrony?

Dostęp do zasobów chmurowych:

- Czy rozumiemy które z przetwarzanych przez nas informacji są dostępne w chmurze obliczeniowej?

Dostęp do zasobów (sieci) klienta i praca zdalna:

- Czy skorzystaliśmy z fachowej pomocy przy konfiguracji dostępu zdalnego do naszej kancelarii i sieci klientów?
- Czy i w jaki sposób korzystamy z prywatnych (domowych) urządzeń w pracy zawodowej?

Prawnik jako doradca podczas cyberincydentu

Materiał dodatkowy

Punkt widzenia – ćwiczenie praktyczne

Na plaży publicznej znajduje się znak „psów wprowadzać nie wolno”. Czy możemy przyjść na plażę z krokodylem ?

- TAK
- NIE

nie ma możliwości odpowiedzenia „to zależy”

Różne grupy zawodowe: prawnicy i informatycy zazwyczaj dość jednoznacznie i zdecydowanie odpowiadają na tak postawiony problem.

Ale udzielają przeciwnych odpowiedzi …

Pamiętajmy o tym w naszej praktyce zawodowej.

Przykład reakcji na incydent

Cyberatak na Centrum Zdrowia Matki Polki w Łodzi

TVN24 | Łódź 3 listopada 2022, 11:49 Autor: pk Źródło: PAP/tvn24.pl

„Dyrektor placówki (…) ostrzega, że skutkiem możliwego wycieku danych osobowych może być m.in. „utrata poufności danych osobowych, chronionych tajemnicą zawodową, utrata danych osobowych powierzonych do przetwarzania Instytutowi na podstawie art. 28 RODO". W związku z tym istnieje wysokie ryzyko „naruszenia praw lub wolności osób fizycznych, których dane dotyczą".

Czy na pewno to jest najważniejsze ryzyko związane z atakiem na systemy IT w szpitalu ?

„Instytut Centrum Zdrowia Matki Polki (ICZMP) padł ofiarą cyberataku. Aby zminimalizować jego skutki, zdecydowaliśmy się na czasowe wyłączenie systemów informatycznych. Prowadzimy intensywne działania, które mają doprowadzić do jak najszybszego, pełnego ich uruchomienia (…) Szpital cały czas stara się prowadzić standardową obsługę pacjentów z wykorzystaniem tradycyjnej dokumentacji. Mimo to nie możemy wykluczyć w najbliższych kilku dniach pewnych utrudnień dla pacjentów. Dlatego apelujemy o wyrozumiałość. O przywróceniu pełnej sprawności systemu informatycznego będziemy informować".

Czy „wyłączenie systemów" to rzeczywiście najlepsza reakcja na tego typu incydent ?

- jeżeli hakerom zależało na danych to na pewno pobrali je zanim atak został wykryty;
- jeżeli celem hakerów był paraliż systemów, to wyłączając je pomogliśmy osiągnąć rezultat;
- przy wyłączonych systemach, jakie kryteria muszą być spełnione by móc uznać że kryzys minął.

Menedżer i prawnik podczas cyberincydentu

Typowe postawy w reakcji na kryzys:

- „zaklinanie rzeczywistości” i deprecjonowanie skali incydentu;
- w reakcji trudności w analizie zdarzenia - poszukiwanie łatwych rozwiązań;
- straty wizerunkowe i chaos komunikacyjny.

Służby IT tracą zaufanie ze strony kierownictwa.

Bardzo często przy kryzysie (także cyberataku) prawnik staje się pierwszym punktem kontaktu dla zarządu - jego ekspertyza jest pomocna, ale oceńmy:

- czy nasza ocena sytuacji uwzględnia szerszy punkt widzenia;
- czy na pewno mamy właściwe kompetencje aby samodzielnie sugerować sposób działania.

Zacznijmy od powołania sztabu kryzysowego skupiającego różnorodne kompetencje.

Co to jest „bezpieczeństwo informacji”

Zgodnie z dobrą praktyką informatyczną bezpieczeństwo identyfikujemy przez trzy atrybuty (cechy):

- **Poufność** (ang. *confidentiality*) - informacja jest udostępniania tylko odbiorcom, którzy są do tego upoważnieni

  Znaczenie terminu może być bardzo szerokie. „Odbiorcami” informacji nie muszą być osoby fizyczne, ale mogą to być instytucje, procesy gospodarcze lub systemy informatyczne

- **Integralność** (ang. *integrity*) - informacja, którą przetwarzamy, nie została zmodyfikowana przez nieuprawnione strony lub w wyniku nieautoryzowanych działań

  Atrybut ten jest często opisywany w powiązaniu z innymi cechami, takimi jak autentyczność, kompletność, rozliczalność czy niezaprzeczalność informacji;

- **Dostępność** (ang. *availibility*) – oznacza, że w zakresie wynikającym z posiadanych przez siebie uprawnień możemy uzyskać w określonym czasie dostęp do żądanych przez siebie informacji

Kombinacja tych 3 atrybutów wystarcza do opisania KAŻDEGO cyberzagrożenia.

W bezpieczeństwie nie zawsze chodzi tylko o zgodność z prawem, a nie wszystkie akty prawne uwzględniają wszystkie powyższe atrybuty.

https://www.linkedin.com/in/jakubbojanowski/

#zdazycprzedhakerem

https://mtbiznes.pl/produkt/zdazyc-przed-hakerem