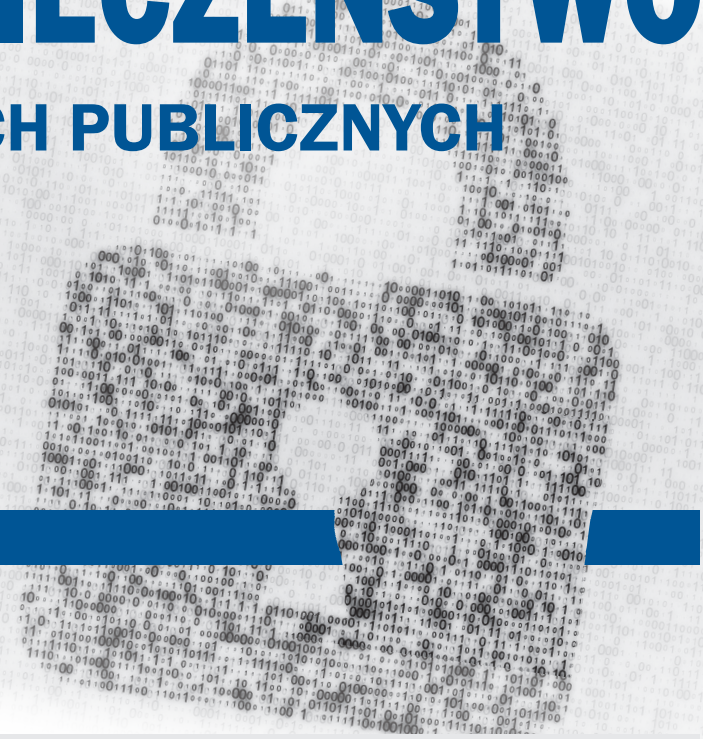
CYBERBEZPIECZEŃSTWO W INSTYTUCJACH PUBLICZNYCH

Zagrożenia i sposoby ochrony



mł. asp. Paweł Tomaszewski

Zakład Służby Kryminalnej CSP

W niniejszym artykule zdefiniowano termin cyberbezpieczeństwo, a także przedstawiono najbardziej popularne zagrożenia z tego obszaru, na które obecnie narażone są instytucje publiczne. Ponadto opisano sposoby postępowania w przypadku wybranych cyberataków oraz metody zapobiegania zagrożeniom systemów informatycznych wykorzystywanych przez te instytucje. Wskazano, że niezmiennie najsłabszym ogniwem obszaru bezpieczeństwa informatycznego jest użytkownik końcowy, czyli człowiek. Podkreślono więc ogromną rolę nieustannych szkoleń dla użytkowników.

Cyberbezpieczeństwo to ramowy termin obejmujący współcześnie swym zakresem ogół wypracowanych praktyk, technik oraz procesów wykorzystywanych dla zapewnienia bezpieczeństwa: układom sieci informatycznych, działającemu w ich środowisku oprogramowaniu czy też zasobom danych gromadzonych i przetwarzanych w ramach baz[1]. Bezpieczeństwo obszaru cyber jest więc ukierunkowane na neutralizację ataków wymierzonych w systemy informatyczne czy też uniemożliwienie intruzowi wszelkich działań pozwalających na nieautoryzowany dostęp do aplikacji[2].

Upraszczając nieco tę kwestię, z punktu widzenia użytkownika końcowego, można stwierdzić, że cyberbezpieczeństwo to niepodatność systemów informatycznych na interakcje prowadzące do złamania standardów obejmujących normy: poufności, integralności, dostępności oraz autentyczności, wykorzystywanych w trakcie konwersji danych.

Kwestia obszaru cyberbezpieczeństwa może być dyskusyjna, jest więc nieco inna z punktu widzenia administratora sieci i użytkownika końcowego, nie ulega jednak wątpliwości, że zarówno jednym, jak i drugim zależy na bezawaryjnej i bezpiecznej pracy systemu informatycznego[3].

Cyberbezpieczeństwo jest stosunkowo nową dziedziną wiedzy, która znajduje zastosowanie w codziennym życiu osób prywatnych, ale jest kluczowa przede wszystkim dla przedsiębiorstw i instytucji. Znajduje do niego pełne zastosowanie ponadczasowa maksyma, która mówi, że lepiej zapobiegać niż leczyć. W zakresie cyberbezpieczeństwa jest naprawdę wiele obszarów, w których należy zachować szczególną ostrożność.

W niniejszym artykule chciałbym skupić się na najbardziej powszechnych aktualnie zagrożeniach dla systemów informatycznych oraz danych należących do instytucji publicznych[4].

ZAGROŻENIE 1. NIEZABEZPIECZENIE DYSKÓW PAMIĘCI URZĄDZEŃ BIUROWYCH

Warto podkreślić, że kardynalnym i nagminnym błędem popełnianym obecnie przez instytucje publiczne w obszarze cyberbezpieczeństwa jest chęć obniżenia kosztów obsługi urządzeń biurowych. Zamiast nabywać sprzęt na własność jest on pozyskiwany w ramach wynajmu czy też opłaty za świadczoną usługę.

Pozornie wszystko jest w porządku, zaoszczędzono pieniądze podatnika, a serwis często psującego się sprzętu spoczywa na dostarczycielu usługi. Jeśli analizujemy tę istotną kwestię, każdemu pracownikowi biurowemu jako pierwsze na myśl przychodzi użytkowanie urządzeń wielofunkcyjnych (drukarka, skaner, kopiarka), których ceny kształtują się często na poziomie kilkunastu czy kilkudziesięciu tysięcy złotych. Oczywiście, nowoczesna technologia i jakość mają wysoką cenę, w tym wypadku bardzo często pomija się jednak kwestię bezpieczeństwa. Współczesne urządzenia wielofunkcyjne mają wbudowane dyski pamięci, które rejestrują treść każdej wykonanej czynności. Tak więc firma zewnętrzna, która w ramach wygranego przetargu świadczy usługi biurowe dla instytucji, pod pretekstem serwisu sprzętu może wymieniać regularnie niniejsze dyski, co potencjalnie daje bezcenną wiedzę, którą można wykorzystać w nielegalny sposób[5]. Informacje z biurowych urządzeń wielofunkcyjnych można pozyskiwać nie tylko metodą fizycznego przejmowania wymiennych dysków, lecz także bardziej wysublimowanymi sposobami, wymagającymi wiedzy fachowej[6]. Jest to możliwe, ponieważ administratorzy w instytucjach bardzo często zapominają o odłączeniu „kombajnów" od publicznego Internetu[7]. Pozostawia to włamywaczowi otwartą furtkę, gdyż często pomijany jest element zapory, która blokuje zarówno przychodzący, jak i wychodzący ruch sieciowy z publicznym Internetem.

Brak wspomnianej zapory zabezpieczającej urządzenie wielofunkcyjne często idzie w parze z brakiem hasła autoryzującego proces drukowania[8]. W instytucjach niejednokrotnie pomija się opcje skonfigurowania urządzenia pod indywidualne potrzeby użytkownika, pozostawiając ustawienia fabryczne, które nadają użytkownikowi szerokie kompetencje, co również stanowi lukę, przez którą można przeprowadzić cyberatak. Czy drukarka obsługuje przesyłanie plików przez FTP? Czy jest to potrzebne w codziennym życiu? Jeśli nie, dobrze gdyby administrator dezaktywował tę funkcję.

ZAGROŻENIE 2. URZĄDZENIA USB

Kolejnym obszarem wielu zagrożeń cyberbezpieczeństwa w instytucjach są urządzenia USB, często mylnie kojarzone jedynie z pendrive'ami. Należy jednak mieć na uwadze, iż w tej grupie urządzeń znajdują się również: zewnętrzne dyski twarde, modemy, aparaty fotograficzne, myszki czy klawiatury. Poprzez ten sprzęt, pozbawiony zabezpieczeń i nadzoru administratora, może dojść do wycieku danych czy zainfekowania komputera złośliwym oprogramowaniem[9].

Administratorzy instytucji publicznych często dalej pozbawieni są komercyjnych programów do monitorowania urządzeń USB, a ze swojej strony nie blokują portów USB, gdyż mocno utrudniałoby to pracę użytkowników końcowych. W dużych firmach prywatnych, gdzie obszar IT jest istotnym filarem działalności przedsiębiorstwa, obecnie często wykorzystuje się oprogramowanie z grupy roboczo zwanej Ekran System, które pozwala na: kontrolowanie i monitorowanie urządzeń USB podłączanych do komputera, otrzymywanie alertów o podłączanych urządzeniach, a także finalnie blokowanie podłączonego urządzenia. Powszechne zastosowanie w instytucjach oprogramowania rodzaju Ekran System nie tylko zabezpieczyłoby je przed wszelkimi wyciekami danych poprzez USB, lecz także dałoby możliwość nagrywania bieżącej działalności na komputerze poszczególnych urzędników, co ułatwiłoby wykrycie ewentualnego wycieku danych czy popełnionego błędu.

Problematyka pamięci przenośnej, dotycząca przede wszystkim pendrive'ów, jest też istotna w odniesieniu do osób, które przychodzą do urzędów załatwić ważną dla nich sprawę, przynosząc dokument zapisany w pliku[10]. W większości przypadków nie zarzucamy petentowi złej woli, jednak dostarczony przez taką osobę nośnik danych może być w różnym stanie technicznym, jak i zainfekowany różnego rodzaju wirusami, a tym samym stanowić zagrożenie dla sprzętu komputerowego instytucji. W skrajnych przypadkach możemy mieć do czynienia z działaniem w złej woli[11] polegającym na przedłożeniu urzędnikowi spreparowanego nośnika, który po włożeniu do portu USB uruchomi funkcję AutoRun, często aktywną na wielu komputerach[12]. Funkcja ta uruchamia się automatycznie w momencie, gdy komputer wykryje obecność dysku USB w porcie USB. W tej samej chwili wirus znajdujący się na dysku USB zostanie przeniesiony i uaktywniony na komputerze biorcy. Jest to skrajnie niebezpieczne, ponieważ urzędnik, który zaufał takiej osobie, nie zdaje sobie sprawy z tego, co naprawdę się wydarzyło. A skala zagrożenia jest szeroka. Przenośne dyski mogą bowiem infekować komputery poprzez konie trojańskie czy złośliwe oprogramowanie umożliwiające dostęp stron trzecich do komputera i informacji.

ZAGROŻENIE 3. DOSTĘP DO INTERNETU I PRACA ZDALNA

Kolejną drażliwą kwestią jest częste bagatelizowanie przez instytucje publiczne środków bezpieczeństwa w trakcie korzystania przez użytkowników końcowych z dobrodziejstw Internetu. Tę lukę bezpieczeństwa w dużej mierze pomniejszyły firmy komercyjne w dobie epidemii Covid-19, kiedy to na szeroką skalę praca przeniosła się z biur do prywatnych mieszkań pracowników. Możliwość wykonywania obowiązków zapewniona była właśnie dzięki sieci Internet. Dla zwiększenia poziomu bezpieczeństwa przesyłania danych zaczęto stosować VPN (*Virtual Private Network*)[13]. VPN z zasady zapewnia bezpieczeństwo sieci i pozwala oszczędzać przepustowość łącz internetowych. Poniżej wymieniono podstawowe zalety korzystania z VPN w środowisku pracy[14].

Korzystanie z VPN zapewnia:

1) **prywatność i anonimowość –** VPN kamufluje prawdziwe IP użytkownika, dokonując jego konwersji na inne zdalne IP, co sprawia, że działania użytkownika w Internecie są dużo trudniejsze do śledzenia, co zwiększa bezpieczeństwo danych;
2) **szyfrowanie danych** – wszystkie pakiety danych przesyłane pomiędzy komputerem użytkownika końcowego a serwerem VPN są szyfrowane, co wyraźnie utrudnia ich przechwycenie, a zarazem odczytanie przez osoby nieuprawnione;
3) **bezpieczne połączenia w publicznych sieciach** – korzystając z publicznych sieci Wi-Fi, w takich miejscach jak urzędy, centra handlowe, dworce, lotniska czy kawiarnie, należy pamiętać o korzystaniu z usługi VPN, gdyż ona znacząco zmniejszy zagrożenia pozyskania naszych danych[15];
4) **bezpieczne przesyłanie plików –** VPN ma szczególną wartość w sytuacji, kiedy mamy do czynienia z przesyłaniem plików zawierających poufne dane, ponieważ zapewnia im zabezpieczenie przed bezprawnym dostępem;
5) **większe bezpieczeństwo pracy zdalnej –** w sytuacjach nadzwyczajnych, w takich jak wspomniana już epidemia Covid-19, VPN zapewnia pracownikom zdalny dostęp do wewnętrznych zasobów i sieci instytucji w sposób dużo bardziej bezpieczny; niestety, obecnie z różnych względów nie we wszystkich instytucjach publicznych wykorzystuje się możliwości sieci VPN[16].

Najlepsze zabezpieczenia zdadzą się jednak na nic, gdy zawiedzie zdrowy rozsądek i dołączy do tego brak elementarnej wiedzy o komputerowym środowisku pracy. Przeprowadzane w urzędach szkolenia z zakresu cyberbezpieczeństwa mają bardzo często charakter formalny, gdyż nie są przeprowadzane od podstaw, a większość uczestników tak naprawdę nie wie, o czym dokładnie jest mowa.

ZAGROŻENIE 4. OSZUSTWO TYPU PHISHING

Polska Policja kilkunastokrotnie odnotowała już zgłoszenia ze strony instytucji, których urzędnicy zostali zręcznie zmanipulowani przez świetnie przygotowanych i poinformowanych oszustów. Głośnym echem odbiła się sprawa z lipca 2013 r., kiedy to oszust podszywający się pod firmę sprzątającą napisał do warszawskiego metra mail informujący o zmianie rachunku bankowego, na który miały być kierowane płatności za wykonane dla metra usługi. Księgowość metra dała się nabrać i w odpowiedzi na prośbę oszusta poprosiła jedynie o wysłanie wniosku w formie pisemnej. Oszust był dobrze przygotowany i przesłał do działu finansów metra tradycyjne pismo zawierające nowy rachunek bankowy dla dokonywania wpłat. Taka inżynieria społeczna zadziałała, nikt z księgowości metra nie zadzwonił do firmy sprzątającej celem weryfikacji całego procesu. W ten sposób w ręce oszusta wpadło 560 000 zł[17].

Do jeszcze bardziej spektakularnego oszustwa doszło w listopadzie 2018 r., gdy to przestępcy podszywający się pod amerykańskiego producenta samolotów, które latają w Polskich Liniach Lotniczych „LOT", przesłali przez Internet do księgowości firmy podrobioną fakturę. Faktura miała na celu wyłudzenie płatności rzekomo za kolejną ratę w ramach realizacji kontraktu. Tym razem na rachunek bankowy oszusta wpłynęło 2 600 000 zł[18].

Taki rodzaj przestępstw nazywany jest potocznie phishingiem, a same ataki przeprowadzane są najczęściej przy pomocy wiadomości e-mail lub SMS. Cyberprzestępcy w tym przypadku podszywają się m.in. pod firmy kurierskie, urzędy administracji, operatorów telekomunikacyjnych, instytucje czy też partnerów biznesowych. Zdecydowana większość phishingu ukierunkowana jest na osoby fizyczne, ale jeśli istnieją szanse zaatakowania z powodzeniem instytucji czy przedsiębiorstwa, to przestępcy na pewno taką próbę podejmą. W wypadku phishingu czynnik ludzki jest kluczowym obszarem jako najsłabsze ogniwo systemu, na który ukierunkowany jest atak[19].

ZAGROŻENIE 5. RANSOMWARE

Inny bardzo poważny obszar zagrożeń dla domeny instytucji publicznych stanowią ataki z grupy ransomware. Ransomware to termin powstały ze zbitki wyrazowej zaczerpniętej z języka angielskiego, łączącej ze sobą dwa terminy: *ransom* – oznaczający okup oraz *software* – tłumaczone jako oprogramowanie. Z punktu widzenia technicznego są to przestępcze działania, których skutkiem jest blokada oraz zaszyfrowanie plików danych znajdujących się na nośnikach danych. Z reguły osobom przeprowadzającym takie działania zależy na wyłudzeniu okupu, co ma być warunkiem przywrócenia stanu uprzedniego danych. Celem takich działań bywają także instytucje publiczne, od których oczywiście trudniej wymusić haracz, jednak perspektywa przedostania się informacji o ataku do mediów publicznych sprawia, że i one często podejmują negocjacje z przestępcami[20].

ZAGROŻENIE 6. ZŁOŚLIWY SPAM

Niestety, sposobów zaatakowania instytucji publicznych jest wiele. Do najpopularniejszych zaliczamy jednak rozsyłanie złośliwego spamu (tzw. malspam), czyli niepożądanych wiadomości służących do rozsyłania szkodliwego oprogramowania. Takie e-maile zawierają szczególnie niebezpieczne elementy w postaci zainfekowanych załączników (np. dokumenty PDF lub Word) lub linków do złośliwych stron. Użytkownik końcowy, wchodząc w zainfekowany link czy otwierając spreparowany załącznik, sam autoryzuje rozpoczęcie ataku na jego system[21].

POSTĘPOWANIE W PRZYPADKU CYBERATAKU

Gdy atak stanie się faktem, nie należy ulegać presji przestępców dążących do zapłaty okupu. Nie ma bowiem żadnej gwarancji, że wywiążą się z warunków postawionych w ramach szantażu, odblokowując dane, ani czy nie zostaną one przez nich wykorzystane do popełniania kolejnych przestępstw. Od strony technicznej zaraz po tym, jak ofiara zorientowała się, że stała się celem ataku, powinna postąpić wedle względnie prostego algorytmu, który przedstawiono poniżej.

ALGORYTM POSTĘPOWANIA w przypadku cyberataku typu ransomware

- **Po pierwsze**, należy odłączyć sprzęt komputerowy od Internetu przy jednoczesnym pozostawieniu włączonego urządzenia, gdyż pamięć urządzenia może zawierać istotne informacje, które będą bardzo pomocne do analizy ataku ransomware[22].
- **Po drugie**, obowiązkowo powinno się zabezpieczyć plik z notatką dot. zaszyfrowania i okupu (ransome note) oraz przykładowe zaszyfrowane pliki.
- **Po trzecie**, należy niezwłocznie skontaktować się z działem IT instytucji i poinformować o zaistniałej sytuacji. Informatycy instytucji powinni zabezpieczyć odpowiednio materiał dowodowy dla organów ścigania oraz podjąć kroki dotyczące zniwelowania skutków ataku. Warto w takim wypadku odwiedzić stronę portalu NoMoreRansom.org, na której być może znajdziemy antidotum w postaci deskryptora, który pozwoli na odszyfrowanie zaatakowanych danych[23]. Ważne jest także, by instytucja, która doświadczyła infekcji systemów, skontaktowała[24] się z CERT NASK[25].

ZAPOBIEGANIE CYBERATAKOM

Naturalnie lepiej jest nie dopuszczać do ataków, niż niwelować ich skutki. Tu jednak muszą ze sobą współdziałać pracownicy działu IT z użytkownikami końcowymi komputerów. Aby czuć się względnie bezpiecznie, pracownicy instytucji publicznych powinni przestrzegać kilku prostych zasad.

Zasady bezpieczeństwa

Po pierwsze – regularnie sporządzać kopię zapasową danych, które znajdują się na komputerach. Ważne jest to, by kopia zapasowa znajdowała się w trybie offline i nie była zagrożona atakiem przeprowadzonym z sieci.
Po drugie – standardem w dzisiejszych czasach jest wspieranie systemów operacyjnych dodatkowym oprogramowaniem antywirusowym.
Po trzecie – żadne oprogramowanie antywirusowe nie będzie działało poprawnie bez aktualizacji i odpowiedniej konfiguracji.
Aż wreszcie **po czwarte** – systematyczne szkolenia użytkowników końcowych pozwolą unikać ewidentnie podejrzanych załączników i linków.

[1] K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, Warszawa 2017, s. 8.
[2] Szacuje się, że okres postępowania w przypadku cyberprzestępstwa wynosi ok. 200 dni, a zaledwie w przypadku 1% z nich zostaje wniesiony akt oskarżenia.
[3] M. Castells, *Społeczeństwo sieci,* Wydawnictwo Naukowe PWN, Warszawa 2008, s. 23.
[4] T. Marciniuk, *Administracja i eksploatacja systemów komputerowych, urządzeń peryferyjnych i lokalnych sieci komputerowych. Podręcznik do nauki zawodu technik informatyk,* Wydawnictwa Szkolne i Pedagogiczne, Warszawa 2019, s. 14.
[5] Tamże, s. 22.
[6] Tamże, s. 23.
[7] Tamże, s. 124.
[8] Hasła – krótkiego, ale silnego i skomplikowanego.
[9] T. Marciniuk, *Administracja i eksploatacja systemów komputerowych, urządzeń peryferyjnych i lokalnych sieci komputerowych. Podręcznik do nauki zawodu technik informatyk,* s. 125.
[10] Tamże, s. 142.
[11] USB Killer – pendrive o właściwościach niszczących płytę główną komputera poprzez zaaplikowanie przez port USB skumulowanego ładunku elektrycznego.
[12] T. Marciniuk, *Administracja i eksploatacja systemów komputerowych, urządzeń peryferyjnych i lokalnych sieci komputerowych. Podręcznik do nauki zawodu technik informatyk*, s. 143.
[13] M. Serafin, *Sieci VPN. Zdalna praca i bezpieczeństwo danych*, Wydawnictwo Helion, Warszawa 2008, s. 18.
[14] Tamże, s. 48.
[15] Tamże, s. 49.
[16] Tamże, s. 152.
[17] Niebezpiecznik, *560 000 PLN wyłudzono od warszawskiego metra*, https://niebezpiecznik.pl/post/560-000-pln-wyludzono-od-warszawskiego-metra/ [dostęp: 27.05.2024 r.].
[18] Business Insider Polska, *Złodzieje oszukali LOT. Linie straciły prawie 2 mln zł, https://businessinsider.com.pl/finanse/lot-oszukany-na-2-mln-zl-przelew-na-zle-konto/c6yghss* [dostęp: 27.05.2024 r.].
[19] J. Jancelewicz, *Socjotechnika, phishing i analiza zdarzeń,* Wydawnictwo Helion, Warszawa 2022, s. 32.
[20] M. Gliwiński, *Ataki na strony internetowe*, Wydawnictwo CSH, Warszawa 2008, s. 18.
[21] Tamże, s. 47.
[22] Tamże, s. 51.
[23] Tamże, s. 55.
[24] NASK, *Kim jesteśmy?*, https://www.nask.pl/? [dostęp: 27.05.2024 r.].
[25] CERT Polska – zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet.

Bibliografia

Business Insider Polska, *Złodzieje oszukali LOT. Linie straciły prawie 2 mln zł, https://businessinsider.com.pl/finanse/lot-oszukany-na-2-mln-zl-przelew-na-zle-konto/c6yghss* [dostęp: 27.05.2024 r.].
Castells M., *Społeczeństwo sieci,* Wydawnictwo Naukowe PWN, Warszawa 2008.
Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, Warszawa 2017.
Jancelewicz J., *Socjotechnika, phishing i analiza zdarzeń*, Wydawnictwo Helion, Warszawa 2022.
Marciniuk T., *Administracja i eksploatacja systemów komputerowych, urządzeń peryferyjnych i lokalnych sieci komputerowych. Podręcznik do nauki zawodu technik informatyk*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 2019.
NASK, *Kim jesteśmy?*, https://www.nask.pl/? [dostęp: 27.05.2024 r.].
Niebezpiecznik, *560 000 PLN wyłudzono od warszawskiego metra*, https://niebezpiecznik.pl/post/560-000-pln-wyludzono-od-warszawskiego-metra/ [dostęp: 27.05.2024 r.].
Serafin M., *Sieci VPN. Zdalna praca i bezpieczeństwo danych*, Wydawnictwo Helion, Warszawa 2008.

Summary

Cybersecurity in public institutions. Threats and ways to protect

This article defines the term ”cybersecurity” as well as presents the most popular threats in this area to which public institutions are currently exposed. Moreover, ways of dealing with selected cyberattacks and methods of preventing threats to the information systems used by these institutions, are described. It was pointed out that the weakest link in the area of cybersecurity is invariably the end user, i.e. the human being. Thus, the huge role of continual user training was stressed.

Tłumaczenie: Katarzyna Olbryś