Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami. Analiza sytuacji i rekomendacje działań

Raport przygotowany przez:

Warszawa, styczeń 2019 r.

Spis treści

1. Wstęp

We współczesnym świecie wraz z rozwojem technologii, cyfryzacji gospodarki i każdego elementu życia społecznego, a przy tym rozwijającej się dynamicznie tzw. infrastruktury krytycznej, zarówno państwowej jak i prywatnej – zmienia się także profil, rodzaj oraz skala obecnych cyberzagrożeń. W ostatnich latach nowym frontem walki z cyberprzestępcami na całym świecie stały się urządzenia końcowe takie jak smartfony, tablety, laptopy, komputery stacjonarne, a nawet drukarki i urządzenia wielofunkcyjne. Dziś sprzęt ten jest niezbędnym elementem funkcjonowania każdej organizacji, firmy czy urzędów państwowych. Jednocześnie jego rosnąca powszechność powoduje, że jest on coraz bardziej wystawiony na ryzyko wykorzystania przez cyfrowych przestępców. Hakerzy bowiem nieustannie szukają najsłabszych elementów i ogniw w firmach oraz administracji publicznej, które są podatne na przeprowadzenie skutecznego cyberataku.

Odpowiednia cyberochrona, szczególnie uwzględniająca właściwy łańcuch dostaw urządzeń końcowych, które byłyby bezpieczne w użytkowaniu i zawierały systemy oraz procedury zabezpieczające przed zagrożeniami cyfrowymi, stała się w ostatnich latach priorytetem wielu rządów, w tym także polskiego. W Polsce kwestia ta została nakreślona w 2017 r. w rządowym dokumencie opisującym krajowe ramy polityki cyberbezpieczeństwa na lata 2017-2022. W 2018 r. rząd podjął pierwszy realny krok w kompleksowym podejściu do cyberbezpieczeństwa w naszym kraju wprowadzając w życie ustawę o Krajowym Systemie Cyberbezpieczeństwa (KSC).

Przedmiotem poniższego raportu jest przedstawienie najważniejszych informacji i szacunków o skali zjawiska cyberataków na urządzenia końcowe na świecie oraz w Polsce oraz wyzwań, jakie czekają zarówno sektor prywatny jak i państwowy w tym zakresie w naszym kraju. Korzystając z doświadczeń firm członkowskich Związku Cyfrowa Polska – światowych liderów najbardziej zaawansowanych technologicznie rozwiązań – poniższa analiza prezentuje również szczegółowe zasady dotyczące cyberbezpieczeństwa urządzeń elektronicznych, które rekomendowane są do wdrożenia zarówno przez biznes, jak i administrację publiczną.

2. Typy cyberataków na urządzenia końcowe

Włamanie się do urządzenia końcowego – smartfonu, tabletu, laptopa, komputera, drukarki lub urządzenia wielofunkcyjnego - podłączonego do firmowej lub urzędniczej sieci, używanego przez pracownika lub urzędnika to prosta droga dla hakera do kradzieży ściśle strzeżonych wewnętrznych danych i informacji, a nawet możliwość zagrożenia funkcjonowania całej organizacji czy ważnej struktury państwa. Aby tego dokonać cyberprzestępcy używają coraz bardziej wyrafinowanych metod, często bazując na nieuwadze i nieostrożności w wykorzystywaniu nowoczesnych urządzeń przez ich użytkowników. Do tych najczęściej stosowanych w ostatnich latach przez hakerów należą:

2.1. Boty oraz wirusy

To automatycznie instalujące się lub nieumyślnie instalowane przez pracownika złośliwe oprogramowania mające na celu przejęcie kontroli nad systemem lub kradzieżą danych. Mogą ono zostać aktywowane, np. w momencie otworzenia wiadomości e-mail lub załącznika do niej lub kliknięcia w link pochodzący z niezweryfikowanego źródła. Cyberprzestępcy „maskują" również złośliwe programy przygotowując pliki udające znane i popularne aplikacje. Hakerzy do osiągnięcia swoich celów coraz częściej wykorzystują też zewnętrzne nośniki, jak dyski, pendrive czy inne urządzenia typu USB.

W 2018 r. istniało około 140 tys. różnego rodzaju wirusów oraz botów

2.2. Phishing i pharming

To w praktyce podszywanie się pod zaufane źródło, np. znaną instytucję lub osobę w celu wyłudzenia poufnych informacji. Phishing wykorzystuje pocztę elektroniczną - cyberprzestępcy rozsyłają maile zachęcające do kliknięcia w link i zalogowania się na podstawionej przez nich stronie, łudzące podobnej do prawdziwej, np. banku, a w efekcie mogą uzyskać dostęp do danych i pieniędzy użytkownika. Natomiast tak samo groźny pharming wykorzystuje przekierowania na fałszywe strony i serwery internetowe, na które jesteśmy kierowani np. poprzez zainstalowane na urządzeniu wirusy i złośliwe oprogramowania.

W 2017 r. ponad 64 proc. przedsiębiorstw na całym świecie doświadczyło ataku phishingowego. 90 proc. dotyczyło wyłudzenia haseł

2.3. Ransomware

To oprogramowanie, które najpierw blokuje dostęp do systemu komputerowego oraz uniemożliwia odczytanie danych, a następnie żąda od użytkownika okupu za przywrócenie stanu pierwotnego. Hakerzy instalują takie oprogramowanie poprzez załącznik w e-mailu lub poprzez przeglądarkę internetową w momencie odwiedzenia strony, która jest zainfekowana złośliwym oprogramowaniem tego typu.

Badania dowodzą, że niemal każda firma i organizacja na świecie była obiektem ataku typu ransomware

2.4. Juice Jacking

To sposób na wykradanie danych ze smartfonów za pomocą „fałszywych" ładowarek do telefonów instalowanych przez hakerów w miejscach publicznych. Tym sposobem cyberprzestępcy z tak podłączonego telefonu mogą nie tylko pobrać dane (zdjęcia, wiadomości, emaile), ale też wgrać na niego złośliwe oprogramowanie.

2.5. Clickjacking

To metoda polegająca na instalowaniu przez hakera złośliwego oprogramowania w określonej aplikacji lub na stronie internetowej (wykorzystując luki w ich zabezpieczeniach). Cyberprzestępcy w niezauważalny dla użytkowników sposób uzyskują dostęp do ważnych przycisków menu na określonej witrynie, którym przypisują własne funkcje i odsyłają na strony przez nich zaprogramowane (gdzie np. znajduje się złośliwe oprogramowanie).

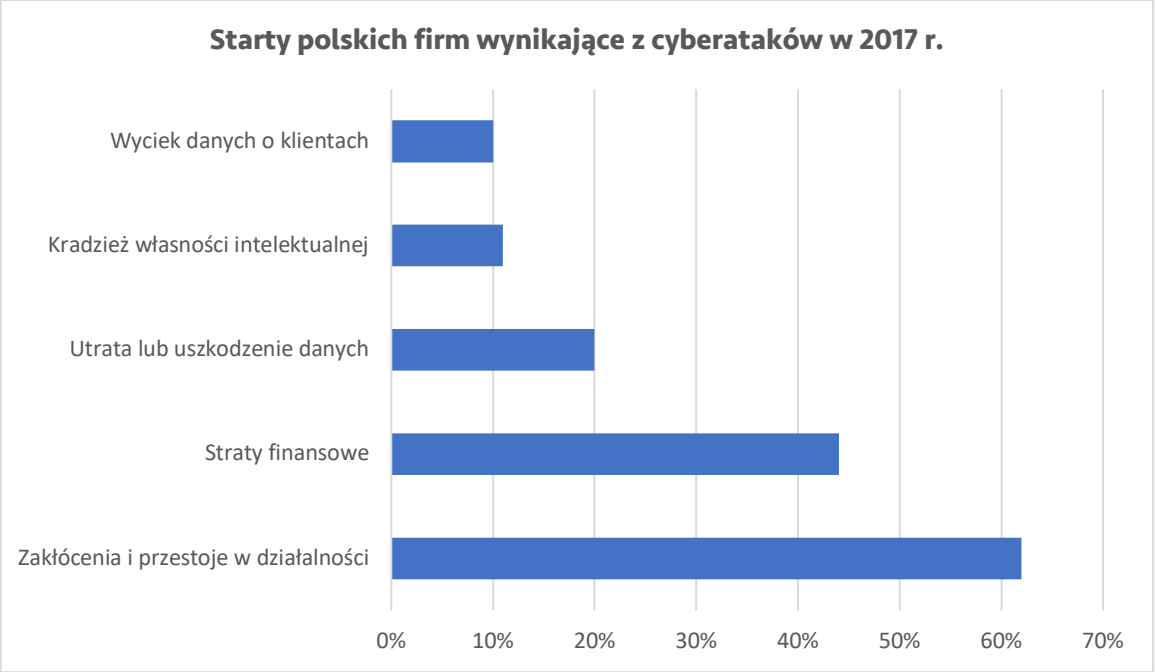
2.6. Man in the middle

Sposób wykorzystywany przez hakerów na podsłuchiwanie i modyfikowanie ruchu sieciowego z urządzenia. Możliwe jest to, np. w sytuacji, gdy użytkownik połączy się z niezaufanym punktem dostępowym do internetu, który zarządzany jest przez hakera. Sposób ten umożliwia m.in. wykradanie danych i haseł.

3. Skala cyberzagrożeń na urządzeniach końcowych

W ciągu ostatnich sześciu latach liczba cyberataków tylko na netbooki i komputery stacjonarne wzrosła na całym świecie o 232 proc[1]. W samej Polsce w 2017 r. podjęto prawie 6 mln prób takich ataków, co oznacza, że średnio 700 razy na godzinę cyberprzestępcy z całego świata starali się włamać się w naszym kraju do prywatnych, firmowych lub państwowych urządzeń i sieci w celu kradzieży informacji i danych[2]. Jednocześnie, jak wynika z przeprowadzonych badań, aż 65 proc. firm w Polsce twierdzi, że w 2017 r. doświadczyło incydentów związanych z zagrożeniem ich bezpieczeństwa[3]. W znacznej części były to ataki typu ransomware.

Konsekwencją rosnących cyberataków są olbrzymie straty ponoszone przez biznes i państwo. W 2015 r. w skali światowej wyniosły one nawet 3 tryliony USD i systematycznie rok do roku wzrastają – szacuje się, że w 2021 r. będą dwukrotnie wyższe i sięgną 6 trylionów USD[4]. W Polsce w 2017 r. w wyniku cyberataków na urządzenia końcowe realne straty finansowe poniosło 44 proc. polskich przedsiębiorstw, a ponad 62 proc. dodatkowo odnotowało zakłócenia i przestoje w swoim funkcjonowaniu, przy czym u 26 proc. przerwa w pracy trwała więcej niż jeden dzień roboczy[5].



[1] Dane firmy Verizon, https://enterprise.verizon.com/resources/reports/dbir/
[2] Dane firmy F-Secure
[3] Raport PwC „Cyber-ruletka po polsku. Dlaczego firmy z cyberprzestępcami liczą na szczęście", 2018 r.
[4] Dane firmy Gartner Inc.
[5] Raport PwC „Cyber-ruletka po polsku. Dlaczego firmy z cyberprzestępcami liczą na szczęście", 2018 r.

Cyberataki doprowadzają już na całym świecie także do poważnych zakłóceń funkcjonowania różnych struktur państwa. Przykładowo w maju 2017 r. doszło do globalnego cyberataku, którego celem były m.in. szpitale w Wielkiej Brytanii, a także sieć telefoniczna w Hiszpanii i wewnętrzna sieć MSW i Komitetu Śledczego w Rosji. Skala ataku typu ransomware o nazwie WannaCry obejmowała w sumie aż 99 krajów. Jedną z pierwszych ofiar WannaCry były szpitala i placówki National Health Service w Anglii, gdzie zablokowano dostęp do komputerów żądając 300 dolarów okupu w BitCoinie w zamian za ich odblokowanie. Część szpitali musiała przełożyć zabiegi, a nowych pacjentów odsyłano do innych placówek. W sumie odwołano ponad 19 tys. wizyt.

Jak wynika ze statystyk, średnio co 4,2 sekundy pojawia się na świecie nowe złośliwe oprogramowanie[6]. Coraz częściej celem ataku hackerów jest hardware urządzeń, na co dowodem jest ostatni raport firmy ESET o ataku na komputery rządowe, do których doszło także w Polsce. Są to szczególnie groźne ataki, gdyż są bardzo trudne do wykrycia i prawie niemożliwe do usunięcia.

Z analiz wynika również, że przestępcy będą w kolejnych latach coraz częściej zainteresowani atakami na urządzenia działające w ramach coraz bardziej ważnego dla biznesu oraz państwa - Internetu Rzeczy (IoT). W 2018 r. odnotowano wyraźny wzrost liczby takich urządzeń, które łączone są z sieciami organizacji, przez co mogą stanowić nowy cel dla atakujących. A według jednej z prognoz, w 2020 roku na świecie będzie nawet 80 milionów urządzeń typu IoT.

Dodatkowo warto zauważyć, że polskie firmy w swoich strategiach coraz częściej stawiają na technologię, która daje im większe szanse i możliwości wzrostu. A to jednocześnie oznacza, że ich działalność wystawiana jest na coraz większe zagrożenia. Nowe kanały sprzedaży on-line, szybsza komunikacja, zwiększona efektywność procesów produkcyjnych osiągnięte dzięki zastosowaniu nowoczesnych rozwiązań IT dają duże pole do działania dla cyberprzestępców.

[6] Raport GData, "Malware Trends 2017", 2017

4. Świadomość cyberzagrożeń w polskich organizacjach

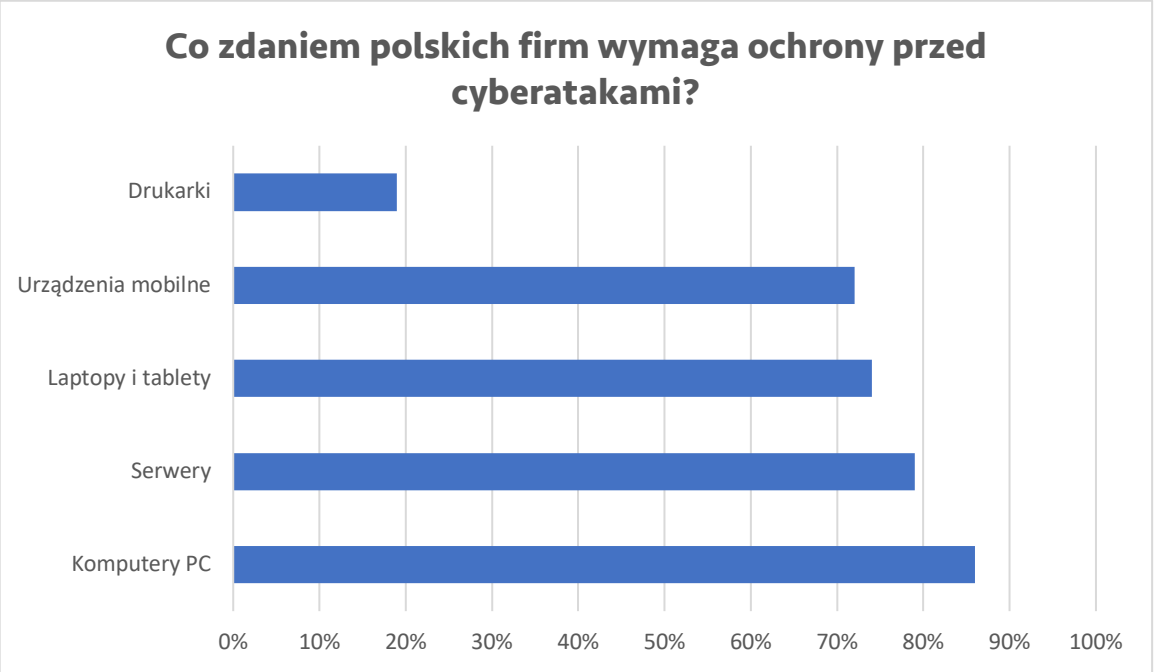
Niestety, jak wynika z różnych dostępnych statystyk i badań przeprowadzonych w ostatnich dwóch latach, wiele organizacji, w tym administracja publiczna, pomimo rosnącej skali cyberataków i wynikających z nich konsekwencji, nadal posiada niedostateczną wiedzę na temat cyberzagrożeń związanych z używaniem urządzeń elektronicznych i nie stosuje odpowiednich zabezpieczeń. Aż 97 proc. organizacji na całym świecie nadal używa przestarzałych technologii cyberbezpieczeństwa[7]. W Polsce tylko 8 na 100 firm jest w pełni zabezpieczona przed cyberatakami, co znaczy, że posiada odpowiednie narzędzia i systemy oraz dedykowany zespół, a także przeznacza odpowiednią część swojego budżetu na inwestycje w tym zakresie (czyli ok. 10 proc. budżetu na IT)[8]. Z badań wynika również, że tylko co 3 smartfon, tablet i laptop w Polsce jest odpowiednio chroniony przed cyberatakami. Tymczasem – jak wynika ze statystyk – na świecie co 53 sekundy kradziony jest laptop mogący zawierać ważne dane[9]. A to oznacza, że bez odpowiednich zabezpieczeń informacje te są dla przestępców łatwo dostępne.

W Polsce nie jest również najlepiej ze świadomością cyberzagrożeń, jakie wiążą się z użytkowaniem urządzeń końcowych. Choć polscy pracownicy deklarują w zdecydowanej większości, że wiedzą, jak zabezpieczać swoje urządzenia elektroniczne, które są wykorzystywane do czynności służbowych, to jedynie 40 proc. z nich w praktyce o tym myśli i stosuje odpowiednie mechanizmy ochronne[10]. Niestety, zabezpieczenia te nie są stosowane do wszystkich urządzeń, które tego wymagają. Z badań wynika, że zdecydowana większość polskich firm uważa, że przed cyberatakami powinny być zabezpieczone przede wszystkim komputery. Gorzej jest z ochroną innych urządzeń podłączonych do firmowej sieci. Nie wszyscy przedsiębiorcy i pracownicy mają świadomość potrzeby ochrony serwerów oraz urządzeń desktopowych i mobilnych. Tylko co 5 przedsiębiorca wie, że cyberochrony potrzebują także drukarki i urządzenia wielofunkcyjne[11]. Tymczasem urządzenie drukujące to bardzo często jedyna część infrastruktury podpięta do firmowej sieci, która ma możliwość komunikacji z każdą stacją roboczą w firmie (niekiedy z ograniczeniem np. do konkretnego piętra lub działu). Oznacza to, że po przejęciu kontroli nad drukarką, z jej adresu IP często można dostać się do zasobów, do których pracownicy niższego szczebla dostępu nie mają. Innymi słowy, drukarkę można wykorzystać do eskalacji uprawnień.

Problemem jest także fakt, że większość systemów bezpieczeństwa dotyka tylko warstwy zewnętrznej, czyli zapewnia bezpieczeństwo na poziomie operacyjnym, a to okazuje się

[7] 2018 Security Raport", Check Point Research
[8] Raport PwC „Cyber-ruletka po polsku. Dlaczego firmy z cyberprzestępcami liczą na szczęście", 2018 r.
[9] Raport firmy Kensington
[10] Badanie Blurred World, Samsung, 2018
[11] Dane *SANS Endpoint Security Survey 2016*

niewystarczające. Jak bowiem wynika ze statystyk najczęstszym źródłem incydentów związanych z bezpieczeństwem są sami pracownicy, a dopiero w dalszej kolejności hakerzy[12].



Z kolei analizując zamówienia publiczne na sprzęt elektroniczny dla polskiej administracji publicznej, można wysunąć wnioski, że również urzędnikom brakuje odpowiedniej wiedzy dotyczącej cyberochrony urządzeń końcowych. Choć od 2016 r. obowiązują Prawo Zamówień Publicznych, które narzuca urzędnikom obowiązek stosowania w postępowaniach przetargowych w dużo szerszym zakresie kryterii pozacenowych, to nawet 90 proc. urzędników przyznaje, że nie do końca wie, jak te zasady zastosować w praktyce i uważa, że potrzebuje na ten temat edukacji. Przy wyborze oferty kierują się oni zatem najczęściej najprostszymi kryteriami poza ceną, takimi jak okres udzielanej gwarancji oraz termin realizacji zamówienia[13]. Kryteria te eliminują jednak najczęściej produkty innowacyjne, spełniające najnowocześniejsze normy dot. cyberbezpieczeństwa.

[12] Raport PwC „Cyber-ruletka po polsku. Dlaczego firmy z cyberprzestępcami liczą na szczęście", 2018 r.
[13] Badanie ARC Rynek i Opinia zrealizowanych przez Związek Cyfrowa Polska oraz UZP, 2017 r.

5. Wnioski i rekomendacje

Kwestie związane z cyberbezpieczeństwem urządzeń końcowych (smartfonów, tabletów, laptopów, komputerów stacjonarnych, drukarek i urządzeń wielofunkcyjnych) w sektorze prywatnym i państwowym to obszar, który wymaga dużych inwestycji oraz edukacji. Wyzwaniem dla firm w najbliższych latach będzie **zapewnienie odpowiedniej cyberochrony swoim przedsiębiorstwom oraz podnoszenie świadomości pracowników w zakresie bezpiecznego wykorzystywania urządzeń końcowych** w wypełnianiu obowiązków służbowych. Wydaje się, że zasadna byłaby tu pomoc państwa, które powinno ułatwić to zadanie polskiemu biznesowi. Konieczne jest wprowadzenie **specjalnych programów lub kampanii edukacyjnych**, które zwiększałyby wiedzę konsumentów o cyberzagrożeniach wynikających ze stosowania smartfonów, tabletów, komputerów stacjonarnych, drukarek czy urządzeń wielofunkcyjnych, a także wskazywały na praktyczne rozwiązania chroniące urządzenia użytkowników przed cyberatakami.

Ponadto jak podkreślono w dokumencie „Krajowe ramy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022" przyjętym przez polski rząd w 2017 roku *„zapewnienie wysokiego poziomu bezpieczeństwa systemów teleinformatycznych wymaga, aby w procesie ich budowania, eksploatacji oraz wycofywania zapewniony był tak zwany bezpieczny łańcuch dostaw"*. Dlatego ważnym zadaniem dla państwa powinno być również stałe kształcenie i podnoszenie świadomości urzędników administracji publicznej z kwestii związanych z bezpieczeństwem cyberprzestrzeni, zwłaszcza w zakresie odpowiedniej i skutecznej ochrony. Szczególnie większą uwagę powinno zwrócić się na edukację w tej kwestii osób odpowiedzialnych za zamówienia publiczne w urzędach i instytucjach publicznych. Docelowo zamawiający urządzenia i usługi, które narażone są na potencjalne cyberataki, powinni dokonywać wyborów takich rozwiązań, które gwarantują bezpieczeństwo cyfrowe. Wymogiem powinno stać się, że **administracja publiczna wykorzystuje tylko taki sprzęt elektroniczny, który posiada specjalny krajowy certyfikat bezpieczeństwa.** Rekomendacja ta zbieżna jest z zapisami rządowej polityki cyberbezpieczeństwa na lata 2017-2022, w których wskazano, że ważnym elementem zapewnienia tzw. bezpiecznego łańcuch dostaw jest ocena i certyfikacja produktów, a priorytetem jest utworzenie „krajowego systemu oceny". Można zgodzić się ze stwierdzeniem zawartym w programie, że będzie to sprzyjać uzyskaniu narodowej niezależności w wymiarze sprzętowym, programistycznym i kryptologicznym.

Istnieje wyraźna potrzeba wypracowania i wdrożenia przez państwo rekomendacji zarówno w zakresie prawa, jak i zabezpieczeń technicznych. Jest to wspólne wyzwanie dla państwa oraz sektora prywatnego – zapewnienie cyberbezpieczeństwa będzie efektywne jedynie przy szerokiej współpracy

ekspertów z doświadczonych firm działających w tym obszarze. Na bazie doświadczeń firm technologicznych będących członkami Związku Cyfrowa Polska opracowano rekomendacje wytycznych w zakresie ochrony urządzeń końcowych przed cyberzagrożeniami, które mogą zostać wdrożone zarówno przez sektor prywatny jak i państwowy. Stanowią one załącznik do tego raportu.

6. Załączniki

- Załącznik nr 1: *Jak minimalizować cyberzagrożenia w użytkowaniu drukarek i urządzeń wielofunkcyjnych?*
- Załącznik nr 2: *Jak minimalizować cyberzagrożenia w użytkowaniu urządzeń mobilnych?*
- Załącznik nr 3: *Jak minimalizować cyberzagrożenia w użytkowaniu laptopów i komputerów stacjonarnych?*

Załącznik nr 1 do Raportu „Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami"

Jak minimalizować cyberzagrożenia w użytkowaniu drukarek i urządzeń wielofunkcyjnych?

Aby zwiększyć bezpieczeństwo drukarek i urządzeń wielofunkcyjnych należy stosować urządzenia, które:

- wyposażone są w mechanizm stałego monitorowania urządzenia na wypadek różnych ataków sieciowych, a w przypadku ich wykrycia możliwość wysłania stosownego komunikatu do zewnętrznego systemu typu SIEM oraz rozpoczęcia procesu eliminacji i zniwelowania potencjalnej próby ataku,
- umożliwiają zablokowanie nieautoryzowanych prób aktualizacji oprogramowania układowego (bios/firmware) oraz możliwość wyłączenia opcji zdalnych aktualizacji, a także wyłączenie portów USB (zarówno dla wydruków z pendrivów, jak również bezpośrednich wydruków z komputera),
- umożliwiają definiowania czasu, po upływie którego urządzenie będzie wylogowywało użytkownika ze strony konfiguracyjnej urządzenia,
- posiadają możliwość automatycznego wylogowania użytkownika z urządzenia po upływie pewnego czasu lub też po wykonaniu zadania,
- umożliwiają zablokowanie dla użytkowników opcji alternatywnego logowania do urządzenia, aniżeli logowanie skonfigurowane jako domyślne,
- posiadają szyfrowanych dyski twarde lub w przypadku ich braku odpowiednio szyfrowane miejsce, w którym przechowywane są dokumenty użytkowników – tymczasowo lub do momentu ich zwolnienia.
- posiadają możliwości zdefiniowania sposobów usuwania danych z urządzenia wraz z nadpisywaniem miejsca, w którym były one zapisane oraz posiadanie mechanizmu trwałego i bezpiecznego usuwania danych z dysku na żądanie.
- posiadają możliwość wymuszenia stosowania przynajmniej PIN-ów w celu wdrożenia poufności drukowanych dokumentów, a w przypadku otrzymania wydruku bez PIN-u – automatycznie go usunąć i pominąć jego drukowanie.

- posiadają możliwości ograniczenia i zdefiniowania docelowych domen pocztowych, na które użytkownicy będą mogli wysyłać swoje skany. Wszystkie pozostałe domeny w adresach email, powinny być zablokowane i ignorowane przez urządzenie,
- posiadają wbudowaną zaporę sieciowa (firewall) lub chociaż możliwość zdefiniowania tzw. listy dostępowej (ACL), czyli komputerów lub serwerów, z których urządzenie będzie tylko przyjmowało dokumenty do wydruku,
- umożliwiają wyłączenie zbędnych i nieużywanych protokołów zarządzania urządzeniem oraz wydruku.
- posiadają wsparcie dla szyfrowanych protokołów transmisji i wydruku,
- posiadają wsparcie dla szyfrowanych protokołów SSL/TLS przy wysyłaniu zeskanowanych dokumentów na maila (SMTP),
- umożliwiają zdefiniowania zblokowanych numerów, z których faksy nie będą odbierane,
- umożliwiają zdefiniowania godzin, w których otrzymane faksy będą drukowane.

Załącznik nr 2 do Raportu „Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami"

Jak minimalizować cyberzagrożenia w użytkowaniu urządzeń mobilnych?

- Budowanie świadomości zagrożeń wśród użytkowników oraz szkolenia z dobrych praktyk w zakresie cyberbezpieczeństwa.
- Stosowanie rozwiązań, które wymuszają szyfrowania danych na urządzeniu oraz zabezpieczenia dostępu do urządzenia za pomocą co najmniej PIN-u, hasła o odpowiednim poziomie skomplikowania lub metod biometrycznych.
- Przechowywanie danych wrażliwych w izolowanym kontenerze będącym oddzielną przestrzenią roboczą zaszyfrowaną sprzętowym kluczem kryptograficznym, wymagającą uwierzytelnienia (na przykład za pomocą biometrii).
- Zapewnienie bezpiecznej transmisji danych z urządzeń mobilnych do systemów zewnętrznych np. poprzez szyfrowane łącze lub stosując rozwiązania VPN.
- Utrzymywanie i w przypadku urządzeń firmowych zdalne wymuszanie aktualnych wersji systemu operacyjnego na urządzeniach na przykład poprzez stosowanie rozwiązań do kontroli wersji oprogramowania.
- W przypadku urządzeń służbowych stosowanie systemów do zarządzania, monitorowania i kontroli urządzeń mobilnych. Oprogramowanie urządzeń mobilnych powinno udostępniać odpowiednie interfejsy dla systemów zarządzania umożliwiające kontrolę wszystkich obszarów wykorzystania urządzeń uwzględniony w polityce bezpieczeństwa firmy.
- Odpowiedni poziom bezpieczeństwa mogą zapewnić tylko sprawdzone rozwiązania dostarczane przez zaufanych i doświadczonych producentów. Przy wyborze rozwiązania należy sprawdzić czy spełnia ono wymagane standardy i normy bezpieczeństwa systemów teleinformatycznych takich jak **Common Criteria (ISO15408).**

Załącznik nr 3 do Raportu „Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami"

Jak minimalizować cyberzagrożenia w użytkowaniu laptopów i komputerów stacjonarnych?

Laptop i komputer stacjonarny powinny posiadać:

- Dysk z funkcją samoszyfrowania SED (*self-encyption drive*) zgodny ze standardem OPAL2.
- W przypadku laptopów i notebooków wbudowana dodatkowa kamera podczerwieni (Infra Red) pozwalająca na bezpieczne logowania do komputera za pomocą skanu twarzy (*face recognition*) z wykorzystaniem wbudowanej technologii Windows Hello.
- Wbudowany kontroler bezpieczeństwa chroniący obszar pamięci EMM przed uruchomieniem na poziomie UEFI nieautoryzowanego kodu złośliwego, będącego wynikiem ataków typy malware.
- W przypadku laptopów i notebooków wbudowany w wyświetlacz filtr prywatyzujący sterowany elektronicznie z klawiatury komputera, pozwalający na ograniczenie kątów widzenia do wartości +/- 45 stopni przy co najmniej 90 proc. spadku kontrastu.