EXATEL

Poradnik podstawowych zasad cyberbezpieczeństwa

Poradnik podstawowych zasad cyberbezpieczeństwa

Materiał edukacyjny przygotowany przez EXATEL S.A.

W tym trudnym dla nas wszystkim czasie, wiele organizacji mierzy się ze zwiększoną falą ataków i zagrożeń w cyberprzestrzeni. Temat cyberbezpieczeństwa jest bardzo obszerny, nie wszyscy jesteśmy w nim ekspertami, jednak **każdy z nas może przyczynić się do zmniejszenia zagrożenia zasobów cyfrowych organizacji przestrzegając kilku podstawowych zasad:**



Jeśli otrzymujesz **maila lub smsa** od **nieznanego nadawcy** – NIE klikaj w załącznik lub link. Zgłoś taką wiadomość do specjalisty od bezpieczeństwa lub IT w Twoim miejscu pracy.



Otrzymując **załącznik lub link od nadawcy**, którego znasz, na wszelki wypadek **przyjrzyj się dokładnie pisowni adresu e-mail i linku.** Często przestępcy wykorzystują adresy podobne – różniące się jedną literą lub innym znakiem – od instytucji, pod które się podszywają, np. banki, urzędy centralne, itp.



Nie udostępniaj danych osobom, których tożsamości nie jesteś w stanie zweryfikować. Jeśli dzwoni do Ciebie ktoś, kto prosi o podanie Twoich haseł dostępu, zrobienie przelewu, przekazanie innych danych, nawet powołując się na polecenie Twojego przełożonego, pamiętaj, że nie możesz mieć pewności kto i w jakim celu próbuje nakłonić Cię do takiego działania.



Nie trzymaj swoich **haseł** dostępu zapisanych **w miejscu łatwo dostępnym** dla osób postronnych. Przy okazji: czy Twoje hasło jest odpowiednio **skomplikowane?** Jeśli korzystasz z hasła w stylu „1234” lub „ImięDataUrodzenia” to lepiej zmień je na coś trudniejszego do odgadnięcia.



Szczególnie teraz, **ogranicz korzystanie z publicznych sieci bezprzewodowych.** Cyberprzestępcy mogą „podszywać się” pod publiczne sieci. Twoją podatność na włamanie do urządzenia zwiększają też uruchomione opcje **Bluetooth** lub **Hotspot**. Jeśli więc akurat nie korzystasz z tych opcji – przełącz je na tryb nieaktywny.



Regularnie **aktualizuj swoje oprogramowanie**, przeglądarki, aplikacje, z których korzystasz. Aktualizacje zwykle aktualizują także opcje ochrony Twojego sprzętu przed atakiem.



Regularnie rób **bezpieczny backup** istotnych dokumentów i informacji. Zapytaj Pracownika IT w Twojej organizacji jakie są wskazane opcje w tym obszarze.

Pamiętaj, że często najsłabszym ogniwem systemu cyberbezpieczeństwa nie jest infrastruktura techniczna lub technologia, tylko człowiek. Szczególnie teraz potrzeba nam uważności i ostrożności, odpowiedzialności za nasze działania.

EXATEL

Czy wiesz jakie są najpopularniejsze **rodzaje ataków na urządzenia mobilne?**





PUBLICZNA SIEĆ WI-FI

Hakerzy mogą zdobywać nasze zaszyfrowane dane poprzez niezabezpieczoną publiczną sieć WiFi. Dlatego nie należy korzystać np. z bankowości online korzystając z publicznej sieci.

APLIKACJE SOCIAL MEDIA

Hakerzy często wykorzystują kanały social media do atakowania swoich ofiar. Podszywają się pod ich konta i rozsyłają do sieci znajomych zainfekowane linki.

ZŁOŚLIWE APLIKACJE

Rozwój konfliktu wojennego w Ukrainie może spowodować dodatkowe zagrożenia związane z cyberbezpieczeństwem, obejmujące aktywność cyberataków, próby wykorzystania luk w systemach, ataki na infrastrukturę sieciową i kampanie dezinformacyjne, zwłaszcza na instytucje publiczne, firmy i infrastrukturę krytyczną.

Organizacje muszą zatem zwiększyć środki ostrożności i ochrony w zakresie cyberbezpieczeństwa, w tym wzmacnianie zabezpieczeń sieciowych, regularne aktualizacje oprogramowania, stosowanie silnych haseł, świadomość pracowników w zakresie zagrożeń cybernetycznych i regularne szkolenia w tym zakresie. Ważne jest również podjęcie działań w celu zapewnienia redundancji danych oraz regularne tworzenie kopii zapasowych, aby móc szybko odzyskać dane w przypadku ewentualnego ataku.

ATAKI WYKORZYSTUJĄCE SMSY

To jeden z najbardziej podstawowych rodzajów ataków hakerskich, który od lat stosują złodzieje, wykorzystując przede wszystkim naszą nieuwagę.

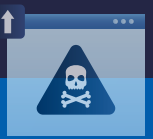
Jak taki atak wygląda? Bardzo prosto. Otrzymujesz SMS z linkiem, który np. informuje o konieczności dopłaty przez Ciebie określonej kwoty do paczki wysłanej kurierem albo weryfikacji Twoich danych na wskazanej, zwykle zaufanej stronie (np. Twojego banku). Niestety ich nadawcą bywają cyberprzestępcy, podszywający się pod znane firmy czy instytucje.

JAKIE SĄ SKUTKI ATAKÓW NA URZĄDZENIA MOBILNE?

Atakujący mogą pozyskać zdjęcia, filmy, nagrania rozmów, dane z mikrofonu w czasie rzeczywistym, dane GPS i lokalizacji, bez jakiejkolwiek interakcji z użytkownikiem urządzenia.

Atakujący mogą sprawić, że telefon komórkowy przestanie działać. W takim przypadku właściciel musi przywrócić urządzenie do ustawień fabrycznych, powodując, że jego cała zawartość zostanie trwale usunięta.

Złośliwe oprogramowania mogą całkowicie ukryć swoją aktywność i sprawić, że nie będzie można ich znaleźć i usunąć z urządzenia mobilnego.



EXATEL



5 największych cyber zagrożeń w życiu codziennym

1 Ataki socjotechniczne

Ataki socjotechniczne wykorzystują interakcje społeczne w celu uzyskania dostępu do cennych danych. U podstaw wszystkich ataków socjotechnicznych leży podstęp. **Cyberprzestępcy podstępem i manipulacją nakłaniają swoje cele do podjęcia określonych działań,** takich jak ominięcie zabezpieczeń lub ujawnienie pewnych poufnych informacji.

2 Nieaktualne oprogramowanie

Wiele ataków spowodowanych jest posiadaniem przestarzałego oprogramowania. Dlatego bardzo istotne jest **aktualizowanie oprogramowania** (na telefonie, komputerze). Gdy tylko atakujący dowiedzą się o luce w oprogramowaniu, mogą ją wykorzystać do przeprowadzenia cyberataku.

3 Ataki na urządzenia mobilne

Technologia mobilna jest bardzo istotnym elementem w naszym życiu codziennym, ale jest także dogodnym polem ataków cybernetycznych. **Większość z tych ataków spowodowana jest złośliwym oprogramowaniem oraz zagrożeniami ze strony publicznych sieci Wi-Fi.**

4 Pośrednicy

Wiele firm, szczególnie w branży retail korzysta z usług stron trzecich, na przykład w zakresie usług przetwarzania płatności. W związku z tym często uważają, że odpowiedzialność za naruszenie danych przez stronę trzecią ich nie dotyczy. W rzeczywistości, **korzystanie z usług dostawcy zewnętrznego nie zwalnia ich z odpowiedzialności za naruszenie danych.**

5 Internet Rzeczy

Internet Rzeczy (IoT) łączy urządzenia wspierające życie codzienne (np. system alarmowy w domu, czy robot sprzątający) za pośrednictwem internetu. Pozwala to na stworzenie sieci urządzeń, które mogą przechowywać, wysyłać i odbierać dane. Ze względu na swoją wygodę, urządzenia typu IoT są coraz częściej wykorzystywane w domostwach. **Należy jednak pamiętać, że hakerzy mogą wykorzystywać łączność internetową jako punkt dostępu do kradzieży danych.**

exatel.pl

EXATEL

Jakie są **rodzaje cyberataków i jak je rozpoznać?**



ROBAKI

To jeden z najczęstszych typów złośliwego oprogramowania.
W przeciwieństwie do wirusów, aktywacja robaków następuje bez świadomości użytkownika, a ich replikacja odbywa się bez wprowadzania zmian w plikach i danych. Robaki rozprzestrzeniają się poprzez luki w oprogramowaniu lub ataki phishingowe.
Gdy robak zainstaluje się w pamięci komputera, zaczyna infekować całe urządzenie, a w niektórych przypadkach nawet całą sieć.

RANSOMWARE

Ataki ransomware polegają na blokadzie lub ograniczeniu dostępu do plików i żądaniu okupu w zamian za ich odzyskanie. O wymierzonym ataku ofiary są informowane na wspólnym ekranie blokady, na którym pojawia się komunikat o konieczności zakupu kryptowaluty, np. Bitcoin'ów do zapłaty okupu. Po jego opłaceniu, ofiary otrzymują klucz deszyfrujący, za pomocą którego mogą odzyskać zablokowane pliki, co niestety nie zawsze kończy się powodzeniem.

MALWARE

Każdy rodzaj złośliwego oprogramowania, którego celem jest uszkodzenie lub wykorzystanie dowolnego urządzenia, aplikacji, usługi lub elementów sieci.
Ataki typu malware są najczęściej rozpowszechniane przez:
- załączniki poczty elektronicznej
- fałszywe reklamy
- zainfekowane aplikacje lub strony internetowe
- linki w smsach i mmsy multimedialne

KOŃ TROJAŃSKI (TROJAN)

Program, który podszywa się pod legalny, godny zaufania plik. Trojany w przeciwieństwie do robaków, potrzebują do aktywacji hosta.
Jeżeli trojan znajdzie się na Twoim urządzeniu, hakerzy mogą go wykorzystać do uzyskania dostępu do Twojej sieci, szpiegowania, usuwania, modyfikacji i przechwycenia danych, a także wykorzystania Twojego komputera jako botneta.

JAK ROZPOZNAĆ, ŻE TWÓJ KOMPUTER ZOSTAŁ ZAINFEKOWANY

- komputer zwalnia działanie i często się zawiesza
- na ekranie pojawiają się dziwne komunikaty
- często dochodzi do awarii systemu
- na komputerze pojawiają się nowe programy, a na pulpicie nieznane dotąd ikony
- zostajesz przekierowany ze znanej ci strony www na zupełnie obcą
- bez twojej zgody tworzą się nowe pliki lub foldery
- w przeglądarce internetowej pojawiają się nowe paski narzędzi
- zmienia się wygląd znanych ci aplikacji i stron, np. głównej strony przeglądarki