# Cyberataki – rodzaje

## 1. Złośliwe oprogramowanie

**Malware** (ang. „malicious software"), to termin określający każdy rodzaj złośliwego oprogramowania, którego celem jest uszkodzenie lub wykorzystanie dowolnego urządzenia, aplikacji, usługi lub elementów sieci. Cyberprzestępcy zazwyczaj wykorzystują malware do pozyskiwania danych, którymi mogą posłużyć się wobec ofiar w celu:

- kradzieży, zaszyfrowania lub usunięcia poufnych informacji
- przejęcia lub zmiany podstawowych funkcji systemu
- monitorowania ich aktywności
- łatwiejszego spamowania użytkowników lub zainstalowania na ich systemie oprogramowania, które wymuszona wizualizację wybranych reklam
- wyłudzania pieniędzy.

**Ataki hakerskie** przy użyciu malware'u są najczęściej rozpowszechniane przez:

- załączniki poczty elektronicznej
- fałszywe reklamy
- zainfekowane aplikacje lub strony internetowe
- linki w smsach i mmsy multimedialne

Aby uniknąć zakażenia złośliwym oprogramowaniem, zapoznaj się z listą najpopularniejszych rodzajów cyberataków przeprowadzanych przy jego użyciu.

To najstarszy rodzaj złośliwego oprogramowania, który **może uszkodzić lub skasować dane na Twoim komputerze**. Aktywuje się po dołączeniu do innego programu lub po uruchomieniu przez użytkownika. Wirus rozprzestrzenia się zazwyczaj poprzez zainfekowane strony internetowe, udostępnianie plików, pobieranie załączników do wiadomości e-mail oraz poprzez fizyczne nośniki danych, takie jak dysk USB. Kiedy dojdzie do zainfekowania, wirus jest w stanie replikować się i rozprzestrzeniać na wszystkie systemy i urządzenia aby wprowadzać zmiany w plikach i danych.

- **Robaki**

To z kolei najczęstszy typ złośliwego oprogramowania. W przeciwieństwie do wirusów, aktywacja robaków nie wymaga dołączania do programu lub uruchamiania przez 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. Wówczas może dojść do modyfikacji i usunięcia plików, infekcji złośliwym oprogramowaniem lub kradzieży danych. Robaki potrafią powielać się w trybie ciągłym, żeby uszczuplić zasoby systemowe, często też instalują przy tym wygodne dla hakerów back doory, które ułatwiają im dostęp do Twoich zasobów.

- **Koń trojański**

Zgodnie z mitologicznym znaczeniem, koń trojański nie jest tym, na co wygląda – w tym przypadku to program, który **podszywa się pod legalny, godny zaufania plik**. Trojany w przeciwieństwie do robaków, do aktywacji potrzebują 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.

- **Ransomware**

Ataki ransomeware polegają na blokadzie lub ograniczeniu dostępu do plików i **żądaniu okupu**
**w zamian za ich odzyskanie**. Początkowo cyberataki przy użyciu ransomeware koncentrowały się na komputerach osobistych, szybko jednak za cel wzięły firmy i organizacje, które są w stanie zapłacić o wiele więcej za odblokowanie krytycznych systemów niż osoby prywatne. 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. Co więcej, hakerzy często instalują złośliwe oprogramowanie w systemie ofiary nawet po zapłaceniu okupu i uwolnieniu danych. Ransomeware należy aktualnie do jednego z największych zagrożeń cyberbezpieczeństwa: do cyberataków za jego pośrednictwem w 2020 roku dochodziło na całym świecie co 14 sekund; w tym roku już co 11 sekund.

- **Adware**

Adware **należy do najbardziej znanej odmiany malware'u. Cyberataki przy jego użyciu polegają na** automatycznym spamowaniu reklamami i generowaniu zysków dla ich autora lub innych, określonych źródeł. W najlepszym przypadku adware jest po prostu irytujący i spowalnia działanie komputera, natomiast w najgorszym, odsyła do stron, które zachęcają do pobrania zainfekowanych plików. Adware może również dostarczać oprogramowanie szpiegujące, przez co urządzenia, na których jest zainstalowane, stają się łatwym celem dla hakerów, phisherów i oszustów. Znane są także przypadki, w których atak Adware był przeprowadzany na zlecenie firm, które chciały w ten sposób zwiększyć swoją sprzedaż.

- **Spyware**

Spyware to oprogramowanie szpiegujące **potajemnie rejestruje aktywność użytkownika w** Internecie, zbierając jego dane i informacje takie jak loginy, hasła i zwyczaje związane z aktywnością w sieci. Hakerzy często wykorzystują je do obserwacji i podsłuchu przez kamery i mikrofony. Spyware jest zwykle rozpowszechniany jako freeware* lub shareware**, który ma atrakcyjną funkcję na froncie i ukrytą przed użytkownikiem misję działającą w tle. Po zainstalowaniu na komputerze spyware przekazuje dane użytkownika reklamodawcom lub cyberprzestępcom, często instalując przy tym dodatkowe złośliwe oprogramowanie, które wprowadza zmiany w ustawieniach. Spyware jest wykorzystywany do kradzieży tożsamości i oszustw związanych z kartami kredytowymi.

***Freeware** jest darmową wersją większego, płatnego programu, publikowaną aby zachęcić potencjalnych klientów do zakupu pełnej wersji. Można go pobierać, instalować, swobodnie używać i udostępniać, ale ze względu na prawa autorskie nie można modyfikować jego kodu źródłowego, ponownie publikować ani integrować z innym oprogramowaniem.

****Shareware** jest natomiast oprogramowaniem dystrybuowanym do potencjalnych klientów na bezpłatny okres próbny (zazwyczaj 30 dni). Jest prawnie ono zastrzeżone i podlega prawom autorskim. Wersje testowe są udostępniane w pełnym wydaniu, lub z częściowo wyłączonymi funkcjami nazywanymi wówczas liteware lub crippleware.

- **Keylogger**

To wersja oprogramowania szpiegującego, polegająca na **przechwytywaniu danych wprowadzanych przez klawiatur**ę. Hasła i numery kart kredytowych, odwiedzane strony internetowe – dane o wszystkim, co wpisujesz trafiają prosto do hakerów, nawet pliki z zrzutami ekranu! Keyloggery są trudne do wychwycenia, wiele z nich posiada bowiem funkcję root-kit, która pozwala im ukrywać się w systemie.

Warto pamiętać, że keyloggery są także użyteczne: np. pomagają działom IT w rozwiązywaniu problemów i monitorowaniu niepowołanych działań użytkowników, a rodzicom w kontrolowaniu aktywności najmłodszych użytkowników. Wszystko zależy więc od tego, jakie intencje ma ten, kto zamierza go użyć.

- **ScareWare**

Jak sama nazwa wskazuje, scareware **straszy i to paradoksalnie infekcją złośliwym oprogramowaniem**. Występuje w formie reklam, banerów i komunikatów, które informują użytkownika o potencjalnym ryzyku zakażenia oraz konieczności wykupienia i instalacji sugerowanego oprogramowania antywirusowego. W najlepszym przypadku jest ono kompletnie bezużyteczne, a w najgorszym może to być np. oprogramowanie ransomeware. Co więcej, scareware atakuje często przez znane, legalne strony internetowe!

## 2. Zaawansowane techniki cyberataków

Malware nie jest oczywiście jedynym sposobem na przeprowadzenie cyberataku. Istnieją również inne, rozmaite techniki, którymi cyberprzestępcy skutecznie atakują swoje ofiary. Do najpopularniejszych należą:

- **DoS** - jest cyberatakiem przeprowadzanym w celu **odcięcia dostępu użytkowników do urządzeń lub sieci**. Ataki DoS polegają zazwyczaj na przeciążeniu lub zalewaniu (flooding) atakowanego obiektu żądaniami, aż do sparaliżowania jego działania i skutkującej tym blokady usług dla użytkowników. Atak DoS jest przeprowadzany za pomocą pojedynczego komputera i łatwo go wykonać z niemal każdego miejsca, dlatego znalezienie sprawcy jest w jego przypadku wyjątkowo trudne.

- **DDoS (Distributed Denial of Service)** to odmiana DoS, która polega na **atakowaniu ofiary z wielu komputerów jednocześnie**. Wykorzystuje określone limity przepustowości zasobów sieciowych, takich jak np. infrastruktura umożliwiająca działanie firmowej strony internetowej; atak DDoS zalewa atakowaną stronę żądaniami tak długo, aż nie będzie ona w stanie ich obsłużyć i zawiesi się.

- **DRDoS (Distributed Reflected Denial of Service) –** to **wzmocniony atak łączący metodę zalewania żądaniami synchronizacji ataku DoS i rozproszonego ataku DDoS**. Polega na zwiększeniu przepustowości ataku bez znacznego zwiększania zasobów atakującego. Przykładowo atakujący przesyła pakiet do usługi, która następnie rozsyła go dalej do kolejnych usług, już bez udziału atakującego.

  Ofiarami ataków DoS padają najczęściej organizacje o wysokim profilu, takie jak **banki, firmy handlowe i medial**ne, a także **organizacje rządowe**. Mimo, że ataki DoS zazwyczaj nie prowadzą do kradzieży lub utraty istotnych informacji lub innych aktywów, mogą kosztować ofiarę dużo czasu i pieniędzy. Nowoczesne techniki cyberbezpieczeństwa wypracowały mechanizmy obrony przed większością form ataków DoS, ale ze względu na unikalne cechy DDoS, jest on nadal uznawany za bardzo groźny.

- **Bot,** czyli **robot internetowy** znany również jako pająk, crawler lub zombie, to **komputer zainfekowany złośliwym oprogramowaniem**, kontrolowany zdalnie przez hakera. Dzięki odpowiednim algorytmom i skryptom, bot jest w stanie w stanie wykonywać polecenia szybciej niż człowiek.

  **Boty** często występują także w postaci złośliwego oprogramowania i mogą być wykorzystywane do wykonywania powtarzających się zadań, takich jak np. indeksowanie wyszukiwarki. Cyberataki przeprowadzane za pośrednictwem botów mają na celu przejęcie całkowitej kontroli nad komputerem ofiary. Kolekcje botów nazywane są botnetami - pomagają hakerom we wszystkich rodzajach cyberataków, są bardzo niebezpieczne, ponieważ rozprzestrzeniają się w sposób niewykrywalny, przez co mogą obejmować nawet miliony urządzeń.

- **Phishing j**est powszechnie stosowanym rodzajem ataku socjotechnicznego. Atakujący p**odaje się za przedstawiciela legalnej instytucji** i kontaktuje się z ofiarą za pośrednictwem e-maila, telefonu lub wiadomości tekstowej, aby nakłonić ją do podania poufnych informacji dotyczących np. kont bankowych i kart kredytowych, loginów oraz haseł. Pozyskane informacje są najczęściej wykorzystywane do przejęcia dostępu do kont użytkownika, co może skutkować poważnymi stratami finansowymi, a nawet kradzieżą tożsamości.

To wyrafinowany rodzaj ataku phishingowego, który może dotknąć absolutnie każdego użytkownika na dowolnej platformie. Wykorzystuje przekierowania na **fałszywe strony i serwery** poprzez zainstalowany na urządzeniu malware, lub luki w oprogramowaniu kontrolującym serwery DNS. Typowa strona phishingowa wygląda dokładnie tak samo jak ta, którą potencjalna ofiara regularnie odwiedza np. robiąc zakupy w sieci. Kiedy użytkownik loguje się na takiej stronie, **hakerzy rozpoczynają przechwytywanie danych**.

- **Atak brute force** to hak kryptograficzny, który polega na **zgadywaniu możliwych kombinacji docelowego hasła**, aż do odkrycia prawidłowego. Im dłuższe hasło, tym atak może być bardziej czasochłonny i trudny do przeprowadzenia - zwłaszcza jeśli ofiara stosuje takie zabezpieczenia jak zaciemnienie danych - a czasami wręcz niemożliwy. Jeśli jednak hasło jest słabe, atak może trwać zaledwie kilka sekund.

To atak kryptologiczny, który można porównać do gry w głuchy telefon, gdzie słowa są przekazywane od uczestnika do uczestnika, aż do momentu, gdy zostaną zmienione przez ostatniego gracza. Środkowy uczestnik manipuluje rozmową przechwytując informacje i dane jej prawowitych uczestników. W trakcie może również wysyłać złośliwe linki lub inne, fałszywe informacje. Niektóre z tych ataków hakerskich potrafią być bardzo wyrafinowane i wręcz niemożliwe do wykrycia, np. kiedy wydaje się, że informacja, którą otrzymujesz pochodzi od Twojego szefa lub kogoś z zespołu.

# Działania prewencyjne

**Jak rozpoznać, że zostałeś zainfekowany złośliwym oprogramowaniem?**

- komputer zwalnia działanie, często się zawiesza
- na ekranie pojawiają się dziwne komunikaty i niedopasowane reklamy (przy powszechnym remarketingu od razu wyda Ci się to podejrzane)
- 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.

**Co wtedy robić?**

Po pierwsze musisz zapobiec rozprzestrzenianiu się infekcji, więc natychmiast wszystko wyłącz: odłącz się od Internetu, Wi-Fi i Bluetooth'a. Spróbuj ustalić jaki to rodzaj infekcji lub ataku – być może będziesz wtedy w stanie naprawić problem i przywrócić pliki za pomocą kopii zapasowej (którą oczywiście posiadasz…? ????). Możesz spróbować ponownie włączyć komputer i przeskanować go za pomocą specjalistycznych programów. Jeżeli boisz się podejmować samodzielnych akcji, skorzystaj z pomocy fachowca, który oczyści komputer i przywróci system.

# Jak chronić się przed cyberatakami?

Niestety w tej kwestii nie ma gotowego rozwiązania, są natomiast dobre praktyki związane z wykrywaniem i blokowaniem ataków hakerskich. Najważniejsze, to abyś przestrzegał kilku podstawowych zasad:

**1. Zainstaluj oprogramowanie antywirusowe i antyspyware**

Programy te skanują pliki komputerowe w celu zidentyfikowania i usunięcia złośliwego oprogramowania. Aby działały poprawnie:

- aktualizuj narzędzia zabezpieczające
- niezwłocznie usuwaj wykryte złośliwe oprogramowanie
- sprawdzaj pliki pod kątem brakujących danych, błędów i nieautoryzowanych dodatków.

**2. Zadbaj o bezpieczne metody uwierzytelniania**

Stosuj znane i sprawdzone metody zabezpieczania kont:

- używaj silnych haseł z co najmniej ośmioma znakami, w tym wielką literą, małą literą, cyfrą i symbolem w każdym haśle
- włącz uwierzytelnianie wieloskładnikowe, takie jak PIN/sms lub pytania zabezpieczające oprócz hasła
- korzystaj z narzędzi biometrycznych, takich jak odciski palców, rozpoznawanie głosu i twarzy
- nigdy nie zapisuj haseł na komputerze, nie przechowuj ich w sieci; w razie potrzeby korzystaj z bezpiecznego menedżera haseł.

**3. Zabezpiecz swoje urządzenia mobilne**

Twój niezabezpieczony, zgubiony lub skradziony telefon daje cyberprzestępcy dostęp do wszystkich przechowywanych w nim danych i zasobów, które mogą zostać użyte nawet do kradzieży tożsamości. Zabezpiecz swoje urządzenia poprzez:

- zainstalowanie oprogramowania antywirusowego
- ustawienie hasła, gestu lub odcisku palca, który należy wprowadzić, aby odblokować urządzenie
- ustawienie w urządzeniu wymogu podania hasła przed zainstalowaniem aplikacji
- ukrycie nieużywanego Bluetooth'a oraz wyłączenie automatycznego łączenia z sieciami
- włączenie funkcji zdalnego blokowania.

**4. Aktualizuj oprogramowanie**

Żaden pakiet oprogramowania nie daje gwarancji zabezpieczenia przed złośliwym oprogramowaniem, jednak producenci regularnie dostarczają poprawki i aktualizacje, aby wyeliminować wszelkie nowe luki w zabezpieczeniach. Jedyne co musisz zrobić to:

- regularnie aktualizuj swoje systemy operacyjne, narzędzia programowe, przeglądarki i wtyczki
- stosuj rutynowe czynności konserwacyjne, aby upewnić się, że oprogramowanie jest aktualne, i sprawdzaj, czy w raportach dzienników nie ma śladów złośliwego oprogramowania.

**5. Stosuj zasadę ograniczonego zaufania**

Uważaj na podstępne e-maile i podejrzane strony internetowe - to potencjalne źródło spamu i phishingu! Pamiętaj:

- nie otwieraj wiadomości z nieznanych adresów e-mail
- wyrzucaj do kosza załączniki z niezapowiedzianych wiadomości
- unikaj ryzykownych kliknięć - zamiast tego wpisuj adresy w przeglądarce
- bądź zawsze gotowy: twórz kopie zapasowe najważniejszych plików, aby ich nie stracić w razie ataku.