Table of Contents

1. Pojęcia cyberbezpieczeństwa 2
1.1. Czym jest cyberbezpieczeństwo 2
1.2. Triada poufności, integralności i dostępności (CIA) 2
1.3. Wybrane podstawowe terminy cyberbezpieczeństwa 7

1. Pojęcia cyberbezpieczeństwa

Projektanci i inżynierowie IoT muszą rozumieć pojęcia z zakresu cyberbezpieczeństwa. Pomaga to zrozumieć różne ataki, jakie mogą zostać przeprowadzone na urządzenia IoT, oraz sposoby wdrażania mechanizmów bezpieczeństwa chroniących je przed cyberatakami. W tym rozdziale omówiono wybrane pojęcia cyberbezpieczeństwa niezbędne do zrozumienia bezpieczeństwa IoT.

1.1. Czym jest cyberbezpieczeństwo

Cyberbezpieczeństwo to technologie, strategie i praktyki mające na celu zapobieganie cyberatakom oraz ograniczanie ryzyka, jakie stwarzają one dla systemów informatycznych i innych systemów cyberfizycznych. Bywa ono nazywane bezpieczeństwem technologii informacyjnych i obejmuje opracowywanie oraz wdrażanie technologii, protokołów i polityk chroniących systemy informatyczne przed kradzieżą danych, ich nielegalną modyfikacją oraz przerwami w działaniu usług. Głównym celem systemów cyberbezpieczeństwa jest ochrona sprzętu, oprogramowania, sieci i danych osób oraz organizacji przed atakami, które mogą naruszyć poufność, integralność i dostępność tych systemów.

Po zrozumieniu, czym jest cyberbezpieczeństwo, należy również wyjaśnić, czym jest cyberatak. Cyberatakiem można nazwać każde celowe naruszenie poufności, integralności lub dostępności systemu informatycznego, czyli nieuprawniony dostęp do sieci, systemu komputerowego lub urządzenia cyfrowego w złośliwym zamiarze kradzieży, ujawnienia, zmiany, wyłączenia lub zniszczenia danych, aplikacji bądź innych zasobów. Udany cyberatak może wyrządzić ofierze poważne szkody – od utraty danych po straty finansowe. Organizacja, której systemy zostały skutecznie zaatakowane, może utracić reputację i zostać zobowiązana do pokrycia szkód poniesionych przez klientów.

Nasuwa się pytanie: dlaczego powinniśmy przejmować się cyberatakami, zwłaszcza w kontekście IoT? Powszechne wykorzystanie IoT do usprawniania procesów biznesowych i poprawy jakości życia wykładniczo zwiększyło możliwości przeprowadzania cyberataków przez przestępców, a tym samym ryzyko dla firm i osób prywatnych. Podkreśla to potrzebę, aby inżynierowie IoT, inżynierowie IT oraz pozostali pracownicy spoza branży IT rozumieli pojęcia cyberbezpieczeństwa.

1.2. Triada poufności, integralności i dostępności (CIA)

Triada CIA to ramy koncepcyjne łączące trzy pojęcia cyberbezpieczeństwa – poufność (ang. *confidentiality*), integralność (ang. *integrity*) i dostępność (ang. *availability*) – w prostą i kompletną listę kontrolną służącą do wdrażania, oceny i doskonalenia systemów cyberbezpieczeństwa. Tworzą one zbiór wymagań, które dobrze zaprojektowany system cyberbezpieczeństwa musi spełniać, aby zapewnić poufność, integralność i dostępność systemów informatycznych. Triada ta stanowi skuteczne narzędzie identyfikacji podatności i zagrożeń w systemach informatycznych, a następnie wdrażania odpowiednich technologii i polityk chroniących te systemy przed kompromitacją. Zapewnia ogólne ramy, którymi kierują się organizacje i eksperci ds. cyberbezpieczeństwa przy projektowaniu, wdrażaniu, ocenie i audycie systemów informatycznych. W kolejnych akapitach krótko omówiono elementy triady CIA (rysunek 1).



Fig. 1: Triada CIA

Poufność

Poufność obejmuje technologie i strategie zapewniające, że wrażliwe dane pozostają prywatne i niedostępne dla osób nieuprawnionych. Oznacza to, że wrażliwe dane mogą być przeglądane wyłącznie przez upoważnione osoby w organizacji i muszą być chronione przed osobami nieupoważnionymi. Część danych zbieranych przez czujniki IoT jest bardzo wrażliwa i nie może być dostępna dla osób o złych zamiarach. Poufność danych obejmuje zestaw technologii, protokołów i polityk zaprojektowanych i wdrożonych w celu ochrony danych przed niezamierzonym, bezprawnym lub nieuprawnionym dostępem, ujawnieniem lub kradzieżą. Aby zapewnić poufność danych, należy odpowiedzieć na następujące pytania:

- Kto powinien móc przeglądać dane lub mieć do nich dostęp?
- Czy istnieją przepisy prawa, regulacje lub umowy wymagające zachowania poufności danych?
- Czy istnieją szczególne warunki, na jakich dane mogą być wykorzystywane lub ujawniane?
- Jak wrażliwe są dane i jakie mogą być konsekwencje uzyskania do nich dostępu przez osoby nieuprawnione?
- Jak cenne mogą być dane dla osób nieuprawnionych (np. cyberprzestępców), jeśli uzyskają do nich dostęp?

Aby zapewnić poufność danych przechowywanych w systemach komputerowych i przesyłanych przez sieci komputerowe i telekomunikacyjne, należy przestrzegać następujących wytycznych:

- Szyfrowanie wrażliwych danych podczas ich przechowywania w systemach komputerowych i przesyłania przez sieci komputerowe i telekomunikacyjne. Szyfrowanie sprawia, że dane stają się nieczytelne lub niezrozumiałe dla osób nieuprawnionych, a odszyfrować je i uzyskać do nich dostęp mogą jedynie posiadacze odpowiednich kluczy. Zastosowany schemat szyfrowania jest utrzymywany w tajemnicy i osoby nieuprawnione nie mają do niego dostępu, chyba że zostanie on skompromitowany.
- Właściwe zarządzanie dostępem do danych, tak aby dostęp do nich miały wyłącznie upoważnione osoby z odpowiednimi uprawnieniami. Użytkownicy powinni zawsze uwierzytelniać się silnymi hasłami, a tam, gdzie to możliwe, należy stosować uwierzytelnianie wieloskładnikowe (np. dwuskładnikowe). Prawa dostępu i uprawnienia użytkowników powinny być regularnie weryfikowane, a zbędne – odbierane.
- Fizyczna lokalizacja systemów sprzętowych i dokumentów papierowych powinna być

odpowiednio zabezpieczona. Tak jak należy kontrolować zdalny dostęp do systemów cyfrowych, tak samo należy ściśle kontrolować dostęp do pomieszczeń, w których przechowywany jest sprzęt i inne krytyczne zasoby. Nawet dokumenty papierowe powinny być właściwie uporządkowane i przechowywane w bezpiecznych miejscach z kontrolowanym dostępem.
- Wszelkie dane, urządzenia sprzętowe i dokumenty papierowe, które nie są już potrzebne, powinny być niezwłocznie i bezpiecznie zutylizowane.
- Należy dbać o to, aby prywatność i poufność danych – zwłaszcza wrażliwych – nie zostały naruszone. Jeśli można obejść się bez zbierania danych wrażliwych, nie należy ich zbierać – jednym ze sposobów uniknięcia ryzyka związanego z przetwarzaniem danych wrażliwych jest niezbieranie ich w ogóle, o ile to możliwe.
- Dane wrażliwe powinny być wykorzystywane tylko wtedy, gdy jest to konieczne; w przeciwnym razie nie należy z nich korzystać, aby zachować ich poufność.
- Należy wdrożyć odpowiednie systemy bezpieczeństwa zapewniające poufność danych. Należą do nich m.in. systemy kontroli dostępu (np. zapory sieciowe), systemy zarządzania zagrożeniami oraz systemy wykrywania i zapobiegania atakom.

Integralność

Integralność w cyberbezpieczeństwie obejmuje technologie i strategie zapewniające, że dane nie zostaną zmodyfikowane ani usunięte przez osoby nieuprawnione podczas przechowywania lub przesyłania. Utrzymanie integralności danych jest niezbędne, aby były one spójne, dokładne i wiarygodne. W kontekście IoT integralność oznacza pewność, że dane zebrane przez czujniki IoT nie zostaną bezprawnie zmienione podczas przesyłania, przetwarzania i przechowywania, co uczyniłoby je niekompletnymi, niedokładnymi, niespójnymi i niewiarygodnymi. Dane mogą być modyfikowane wyłącznie przez osoby uprawnione do dostępu do nich. Zebrane dane muszą pozostać kompletne, dokładne, spójne i bezpieczne przez cały cykl życia, w następujący sposób [1)]:

- Aby zapewnić kompletność, dane muszą być przechowywane w pełnej postaci, bez odfiltrowania, obcięcia lub utraty jakichkolwiek elementów.
- Dokładność danych zachowuje się, dbając o to, aby nie zostały one zmienione ani zagregowane – w wyniku błędu ludzkiego lub złośliwego ataku – w sposób wpływający na wyniki dalszego przetwarzania i analizy.
- Spójność danych należy utrzymywać, zapewniając, że dane pozostają niezmienione niezależnie od tego, jak często są odczytywane i jak długo są przechowywane.
- Bezpieczeństwo danych należy zapewnić, gwarantując, że są one bezpiecznie przechowywane i dostępne wyłącznie dla uprawnionych aplikacji i osób. Metody ochrony danych, takie jak uwierzytelnianie, autoryzacja, szyfrowanie czy kopie zapasowe, pozwalają zapobiec zmianie lub zniszczeniu danych przez nieuprawnione aplikacje lub osoby.

Projektanci, producenci, deweloperzy i operatorzy systemów IoT powinni dbać o to, aby zebrane dane nie zostały utracone, ujawnione ani uszkodzone podczas przesyłania, przetwarzania lub przechowywania. Ponieważ ilość danych zbieranych przez czujniki IoT rośnie, a wiele firm opiera decyzje na wynikach ich przetwarzania, zapewnienie integralności danych ma kluczowe znaczenie. Należy zagwarantować, że zebrane dane IoT są kompletne, dokładne, spójne i bezpieczne przez cały cykl życia, ponieważ dane skompromitowane mają dla organizacji i użytkowników niewielką wartość lub nie mają jej wcale. Niepożądane są również utraty danych wynikające z błędów ludzkich i cyberataków. Na integralność danych mogą wpływać czynniki fizyczne i logiczne.

- Integralność fizyczna: obejmuje różne sposoby, w jakie integralność danych może zostać naruszona podczas przesyłania, przechowywania i odczytu. Podczas transmisji część danych może zostać utracona wskutek utraty pakietów w urządzeniach sieciowych lub błędów pakietów spowodowanych zakłóceniami w medium transmisyjnym. Dane mogą również zostać utracone w

wyniku fizycznego uszkodzenia urządzeń pamięci masowej lub urządzeń obliczeniowych.
Integralność danych może zostać naruszona z następujących powodów:
- Awarie i usterki sprzętu.
- Błędy projektowe i zaniedbania.
- Naturalne awarie wynikające z degradacji urządzenia (np. korozji).
- Awarie i przerwy w zasilaniu.
- Klęski żywiołowe.
- Awarie wywołane czynnikami środowiskowymi, np. ekstremalnie wysoką temperaturą.
- Cyberataki mające na celu wywołanie awarii sprzętu lub zasilania (np. ataki wyczerpujące energię).

Fizyczną integralność danych można zapewnić poprzez:

- Wdrożenie redundancji w systemach przechowywania danych, tak aby awaria jednej pamięci nie powodowała utraty danych.
- Zastosowanie pamięci podręcznej zapisu z podtrzymaniem bateryjnym.
- Stosowanie systemów pamięci masowej z zaawansowanymi pamięciami z korekcją błędów.
- Wdrożenie klastrowych i rozproszonych systemów plików.
- Stosowanie algorytmów wykrywania błędów w celu wykrycia zmian w danych podczas transmisji.
- Tworzenie kopii zapasowych przechowywanych w różnych lokalizacjach fizycznych.
- Wdrożenie mechanizmów ochrony sieci zapewniających, że dane nie zostaną uszkodzone ani utracone podczas przesyłania.

Projektanci, producenci i deweloperzy systemów IoT mogą stosować różne technologie i polityki zapewniające integralność sprzętu – od urządzeń IoT, przez komunikację, po centra danych mgły/chmury.

- Integralność logiczna: nawet przy braku problemów ze sprzętem mogą wystąpić niezamierzone lub złośliwe zmiany danych bądź ich utrata podczas przesyłania, przechowywania i odczytu, naruszające ich integralność. Integralność logiczną mogą naruszyć błędy projektowe oprogramowania, błędy w kodzie, niewłaściwa konfiguracja sieci, błędy ludzkie i cyberataki. Do zagrożeń dla integralności danych należą m.in.:
  - Dane mogą zostać usunięte, błędnie wprowadzone lub bezprawnie zmienione w systemie przechowywania.
  - Dane mogą zostać uszkodzone, utracone lub bezprawnie zmienione podczas przesyłania.
  - Dane mogą zostać skradzione, uszkodzone lub bezprawnie zmienione przez złośliwego hakera po udanym cyberataku.
  - Niewłaściwa konfiguracja sieci i infrastruktury może doprowadzić do kradzieży, uszkodzenia, utraty lub bezprawnej zmiany danych.

Zapewnienie integralności danych jest złożonym zadaniem, wymagającym starannej integracji narzędzi cyberbezpieczeństwa, polityk, regulacji i ludzi. Do sposobów zapewnienia integralności danych należą m.in. następujące strategie:

- Dostęp do danych powinien być ściśle kontrolowany za pomocą skutecznych narzędzi uwierzytelniania i autoryzacji, aby osoby nieuprawnione nie mogły nimi manipulować.
- Należy tworzyć i starannie audytować dzienniki działań użytkowników, aby śledzić wprowadzane przez nich zmiany.
- Dane powinny być szyfrowane podczas przesyłania i przechowywania, aby nie zostały zmienione ani uszkodzone.
- Należy stosować mechanizmy ochrony danych zapobiegające ich utracie, np. regularnie

wykonywać kopie zapasowe oraz stosować algorytmy komunikacyjne z wykrywaniem i korekcją błędów.
- Podczas uzyskiwania dostępu do danych w celu ich przetworzenia lub analizy należy podjąć niezbędne kroki, aby nie zostały one uszkodzone, utracone lub zniszczone – zwłaszcza gdy korzystają z nich podmioty trzecie.
- Pracownicy i inni interesariusze powinni zostać przeszkoleni w zakresie postępowania z danymi tak, aby nie naruszyć ich integralności.

Dostępność

Systemy obliczeniowe, komunikacyjne oraz systemy przechowywania i odczytu danych powinny być dostępne w dowolnym momencie, gdy są potrzebne. Dostępność w kontekście cyberbezpieczeństwa to możliwość niezawodnego uzyskania dostępu do systemów informatycznych przez uprawnionych użytkowników lub aplikacje w dowolnym momencie, gdy jest to konieczne. Jest to jeden z elementów triady CIA, stanowiący wymaganie przy projektowaniu bezpiecznych i niezawodnych systemów informacyjno-komunikacyjnych, takich jak IoT. Ponieważ węzły IoT są integrowane z infrastrukturą krytyczną oraz inną istniejącą infrastrukturą firm i osób prywatnych, dłuższe przestoje są niedopuszczalne, co czyni dostępność wymaganiem kluczowym. Utrata dostępności może wynikać z następujących przyczyn:

- Awarie sprzętu, w tym wynikające z naturalnej degradacji.
- Awarie oprogramowania wynikające z błędów projektowych lub błędów w kodzie.
- Cyberataki, np. DoS/DDoS lub – w przypadku węzła IoT – atak wyczerpujący energię.
- Awaria zasilania wynikająca z przerw w dostawie energii lub – w przypadku węzłów IoT – wyczerpania energii zgromadzonej w baterii.
- Uszkodzenie lub utrata danych podczas przesyłania, przechowywania lub odczytu, uniemożliwiające uprawnionym użytkownikom i aplikacjom dostęp do danych, gdy są potrzebne.
- Wąskie gardła przepustowości i awarie łączy w sieci komunikacyjnej, zakłócające przesyłanie danych do użytkowników i aplikacji.
- Przestoje wynikające z awarii, nieprawidłowego zachowania lub wadliwego działania samych systemów cyberbezpieczeństwa.
- Szkody w infrastrukturze obliczeniowej, komunikacyjnej i pamięci masowej spowodowane klęskami żywiołowymi, kradzieżą, wandalizmem, niepokojami politycznymi lub konfliktami.

Do sposobów zapewnienia dostępności systemów informatycznych i danych należą m.in.:

- Tworzenie kopii zapasowych danych i przechowywanie ich w różnych lokalizacjach geograficznych.
- Zapewnienie skutecznych procesów eksploatacji i utrzymania.
- Zapewnienie wydajnych i niezawodnych źródeł energii oraz systemów jej magazynowania.
- Minimalizacja zużycia energii w celu wydłużenia czasu życia węzłów IoT.
- Szybkie usuwanie błędów projektowych i błędów oprogramowania w celu minimalizacji przestojów.
- Staranne zabezpieczenie fizycznych lokalizacji infrastruktury sprzętowej.
- Skuteczne mechanizmy uwierzytelniania i autoryzacji, zapewniające uprawnionym użytkownikom dostęp do systemów, gdy jest potrzebny.
- Staranne wdrożenie i konfiguracja systemów cyberbezpieczeństwa w celu minimalizacji spadku wydajności i przestojów wynikających z ich wadliwego działania.
- Zapewnienie prawidłowej konfiguracji systemów sieciowych z odpowiednimi mechanizmami bezpieczeństwa oraz szybkie usuwanie awarii sieci.

1.3. Wybrane podstawowe terminy cyberbezpieczeństwa

Aby zrozumieć zaawansowane pojęcia i technologie cyberbezpieczeństwa, trzeba dobrze znać pojęcia podstawowe. Poniżej przedstawiono wybrane z nich.

Ryzyko cyberbezpieczeństwa: prawdopodobieństwo narażenia na cyberatak lub naruszenia któregokolwiek z wymagań poufności, integralności lub dostępności, co może skutkować kradzieżą, wyciekiem, uszkodzeniem lub zniekształceniem danych. Może ono również prowadzić do zakłóceń lub przestojów usług, w wyniku których firma traci przychody, a infrastruktura ulega uszkodzeniu. Organizacja, która padła ofiarą udanego cyberataku, może stracić reputację i zostać zobowiązana do wypłaty odszkodowań klientom lub zapłaty kary organom nadzorczym. Ryzyko cyberbezpieczeństwa to zatem potencjalne straty, jakie organizacja lub osoby mogą ponieść w wyniku udanych cyberataków lub awarii systemów informatycznych, prowadzących do utraty danych, klientów, przychodów i zasobów (aktywów oraz strat finansowych).

Zagrożenia: działanie podejmowane w celu naruszenia któregokolwiek z wymagań cyberbezpieczeństwa, które może skutkować kradzieżą, wyciekiem, uszkodzeniem, zniekształceniem lub utratą danych. Działanie takie może ujawnić dane osobom nieuprawnionym lub bezprawnie je zmienić. Może też prowadzić do zakłócenia usług wskutek przestoju systemu, jego niedostępności lub niedostępności danych. Zagrożenia obejmują m.in. infekcje urządzeń wirusami lub złośliwym oprogramowaniem, ataki ransomware, odmowę usługi, phishing, ataki socjotechniczne, ataki na hasła, wstrzykiwanie SQL, naruszenia ochrony danych, ataki typu man-in-the-middle, ataki wyczerpujące energię (w przypadku urządzeń IoT) i wiele innych wektorów ataku. Zagrożenia cyberbezpieczeństwa mogą pochodzić od takich podmiotów jak państwa, cyberprzestępcy, haktywiści, niezadowoleni pracownicy, a także wynikać z błędów projektowych, błędnej konfiguracji systemów, wad lub błędów oprogramowania, działań terrorystów i szpiegów, błędów uprawnionych użytkowników oraz klęsk żywiołowych [2)].

Podatność: słabość, wada lub błąd w systemie informatycznym lub systemie cyberbezpieczeństwa, który cyberprzestępcy mogą wykorzystać do naruszenia bezpieczeństwa systemu. Istnieje wiele podatności i wciąż odkrywane są nowe. Do najczęstszych należą wstrzykiwanie SQL, przepełnienie bufora, cross-site scripting, błędna konfiguracja zabezpieczeń [3)], słabe mechanizmy uwierzytelniania i autoryzacji oraz niezaszyfrowane dane podczas przesyłania lub przechowywania. Podatności można identyfikować za pomocą skanerów podatności i testów penetracyjnych. Po wykryciu podatności należy podjąć kroki w celu jej usunięcia lub ograniczenia związanego z nią ryzyka.

Exploit: różne sposoby wykorzystywania przez cyberprzestępców podatności do przeprowadzania cyberataków naruszających poufność, integralność i dostępność systemów informatycznych. Exploit może obejmować zaawansowane techniki (np. polecenia, skrypty lub programowanie) oraz narzędzia programowe (komercyjne lub otwartoźródłowe) służące do identyfikacji i wykorzystania podatności w celu kradzieży danych, zakłócenia usług, uszkodzenia danych lub przejęcia danych bądź systemów w zamian za okup.

Wektor ataku: różne sposoby, w jakie atakujący mogą naruszyć bezpieczeństwo systemu informatycznego, np. systemów obliczeniowych, komunikacyjnych lub systemów przechowywania i odczytu danych. Do typowych wektorów ataku należą:

- Ataki phishingowe.
- Załączniki poczty elektronicznej.
- Kradzież danych uwierzytelniających z użyciem różnych technik socjotechnicznych.
- Przejęcie konta w celu kradzieży lub zniszczenia danych i innych zasobów oraz przeprowadzenia

dalszych ataków.
- Kryptoanaliza zaszyfrowanych danych.
- Ataki typu man-in-the-middle.
- Cross-site scripting.
- Wstrzykiwanie SQL.
- Zagrożenia wewnętrzne.
- Wykorzystanie podatności (np. w niezałatanym oprogramowaniu, serwerach i systemach operacyjnych).
- Ataki przez przeglądarkę, kompromitacja aplikacji.
- Ataki siłowe (brute-force) na hasła.
- Wykorzystanie złośliwego oprogramowania do przejęcia urządzeń, uzyskania nieuprawnionego dostępu i wyrządzenia szkód w danych lub systemach.
- Wykorzystanie otwartych portów.

Do sposobów eliminowania wektorów ataku w celu zmniejszenia szans na udany atak należą [4)]:

- Szyfrowanie danych podczas przesyłania, przechowywania i odczytu.
- Opracowanie skutecznych polityk bezpieczeństwa oraz szkolenie pracowników i interesariuszy i egzekwowanie ich stosowania.
- Łatanie podatności poprzez regularne aktualizacje oprogramowania i sprzętu oraz kontrolę konfiguracji systemów.
- Wdrożenie bezpiecznych mechanizmów dostępu do sieci.
- Regularne audyty bezpieczeństwa w celu wykrycia i usunięcia zagrożeń i podatności, zanim wykorzystają je cyberprzestępcy.
- Wdrożenie systemów wykrywania i zapobiegania zagrożeniom (włamaniom).

Powierzchnia ataku: miejsca lub możliwe wektory ataku, które cyberprzestępcy mogą wykorzystać do naruszenia poufności, integralności i dostępności danych i systemów informatycznych. Organizacje i osoby prywatne powinny dążyć do minimalizacji swojej powierzchni ataku – im jest ona mniejsza, tym mniejsze prawdopodobieństwo kompromitacji danych lub systemów. Dlatego należy stale monitorować powierzchnię ataku, aby jak najszybciej wykrywać i blokować ataki oraz minimalizować ryzyko ich powodzenia. Typowe elementy powierzchni ataku to słabo zabezpieczone urządzenia (np. komputery, telefony komórkowe, dyski twarde i urządzenia IoT), słabe hasła, brak zabezpieczeń poczty elektronicznej, otwarte porty oraz nieinstalowanie poprawek oprogramowania, co otwiera atakującym „tylne drzwi”. Inną typową powierzchnią ataku są słabe protokoły webowe, które hakerzy mogą wykorzystać do kradzieży danych w atakach man-in-the-middle (MITM). Wyróżnia się dwie kategorie powierzchni ataku [5)]:

- **Cyfrowa powierzchnia ataku**: obejmuje wszystkie systemy programowe i sprzętowe w infrastrukturze organizacji, w tym aplikacje, kod, porty, serwery, strony internetowe i urządzenia sensorowe (urządzenia IoT). Przy wdrożeniach obejmujących dziesiątki lub setki milionów urządzeń IoT powierzchnia ataku tworzona przez infrastrukturę IoT – od warstwy czujników, przez infrastrukturę sieciową, po infrastrukturę obliczeniową mgły/chmury – jest ogromna.
- **Fizyczna powierzchnia ataku**: obejmuje wszystkie urządzenia końcowe, do których atakujący może uzyskać fizyczny dostęp, takie jak komputery stacjonarne, dyski twarde, laptopy, telefony komórkowe, pamięci USB oraz (w przypadku systemów IoT) urządzenia IoT. Do fizycznej powierzchni ataku należą m.in. niedbale wyrzucony sprzęt zawierający dane użytkowników i dane logowania, hasła zapisane na kartkach oraz nieuprawniony dostęp do miejsc, w których przechowywane są wrażliwe zasoby.

Skuteczne zarządzanie powierzchnią ataku zapewnia organizacjom i osobom następujące korzyści:

- Identyfikacja i usuwanie podatności.
- Ograniczanie ryzyka związanego z zagrożeniami cyberbezpieczeństwa.
- Identyfikacja nowych elementów powierzchni ataku powstających w miarę rozbudowy infrastruktury i wdrażania nowych usług.
- Skuteczne zarządzanie dostępem do krytycznych zasobów i danych, minimalizujące ryzyko naruszenia bezpieczeństwa.
- Minimalizacja prawdopodobieństwa udanych cyberataków.

W miarę jak infrastruktura IT rośnie i łączy się z zewnętrznymi systemami przez Internet, staje się coraz bardziej złożona, trudniejsza do zabezpieczenia i częściej atakowana. Do sposobów minimalizacji powierzchni ataku i ograniczenia ryzyka cyberataków należą:

- Wdrożenie polityk zero-trust, zapewniających, że dostęp do zasobów informacyjnych (urządzeń obliczeniowych, czujników, sieci, serwerów, baz danych itp.) mają wyłącznie uprawnieni użytkownicy i aplikacje. Eliminuje to lub ogranicza możliwość nieuprawnionego dostępu.
- Ograniczenie zbędnej złożoności poprzez wyłączenie lub usunięcie nieużywanego sprzętu i oprogramowania z infrastruktury IT, co zmniejsza powierzchnię ataku.
- Regularne audyty bezpieczeństwa i skanowanie całej sieci i systemów IT w celu identyfikacji i usunięcia podatności (sprzętowych i programowych), które mogliby wykorzystać cyberprzestępcy.
- Podział sieci na mniejsze segmenty za pomocą zapór sieciowych i mikrosegmentacji, co tworzy dodatkowe bariery, ogranicza rozprzestrzenianie się ataków i zmniejsza powierzchnię ataku.
- Regularne szkolenie pracowników, aby stosowali dobre praktyki bezpieczeństwa i przestrzegali polityk bezpieczeństwa danych i systemów informatycznych.

Szyfrowanie: przekształcanie danych w tajny kod (dane zaszyfrowane), który może zostać przekształcony z powrotem do postaci pierwotnej (odszyfrowany) wyłącznie za pomocą unikalnego klucza przez uprawnionych użytkowników lub aplikacje. Szyfrowanie chroni poufność i integralność danych, tzn. zapobiega ich kradzieży lub bezprawnej zmianie przez cyberprzestępców. Stosuje się je do ochrony danych podczas przesyłania, przechowywania i przetwarzania/analizy. Proces szyfrowania polega na użyciu matematycznego algorytmu kryptograficznego (algorytmu szyfrującego) do przekształcenia danych (tekstu jawnego) w szyfrogram, który można przekształcić z powrotem w tekst jawny jedynie za pomocą innego algorytmu (algorytmu deszyfrującego) i odpowiedniego unikalnego klucza. Klucze kryptograficzne powinny być na tyle długie, aby cyberprzestępcy nie mogli ich łatwo odgadnąć atakiem siłowym lub kryptoanalizą. Cele stosowania algorytmów szyfrowania w systemach informatycznych to:

- Zapewnienie poufności danych – uniemożliwienie dostępu do nich osobom nieuprawnionym i zachowanie ich w tajemnicy.
- Zapewnienie integralności danych – zagwarantowanie, że nie zostaną zmienione, uszkodzone ani zniekształcone podczas przechowywania lub przesyłania.
- Uwierzytelnianie użytkowników poprzez weryfikację pochodzenia danych, tak aby mieć pewność, że użytkownicy są tymi, za kogo się podają.
- Zapewnienie niezaprzeczalności – nadawca danych nie może zaprzeczyć, że jest ich źródłem.
- Umożliwienie organizacjom spełnienia wymagań regulatorów, którzy nakazują odpowiednią ochronę danych wrażliwych przed kradzieżą, uszkodzeniem i bezprawną modyfikacją.

Algorytmy kryptograficzne dzielą się na dwa główne rodzaje:

- **Szyfrowanie symetryczne**: ten sam klucz służy do szyfrowania i deszyfrowania, dlatego bywa ono nazywane szyfrowaniem z kluczem prywatnym lub współdzielonym. Klucz przesyła się bezpiecznym kanałem, aby można go było użyć do odszyfrowania danych. Główną zaletą tego

schematu jest stosunkowo niski koszt utworzenia szyfrogramu, co czyni go mniej kosztownym obliczeniowo i szybszym w deszyfrowaniu. Istotną wadą jest możliwość kompromitacji klucza podczas jego przekazywania od nadawcy do odbiorcy. Jeśli klucz pozna strona trzecia, osoba lub aplikacja może go użyć do odszyfrowania danych, naruszając ich poufność i integralność. Przykładami algorytmów symetrycznych są Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES) i Twofish.
- **Szyfrowanie asymetryczne**: do szyfrowania i deszyfrowania używa się dwóch różnych kluczy (prywatnego i publicznego), dlatego bywa ono nazywane szyfrowaniem z kluczem publicznym. Klucz publiczny jest udostępniany stronom komunikacji (nadawcom) do szyfrowania danych, ale odszyfrować je może tylko odbiorca posiadający odpowiedni klucz prywatny. Algorytmy asymetryczne są stosunkowo bezpieczne, ale generowanie szyfrogramu jest względnie kosztowne, a deszyfrowanie wymagające obliczeniowo. Przykładami algorytmów z kluczem publicznym są RSA (Rivest-Shamir-Adelman) i kryptografia krzywych eliptycznych (ECC).

Choć szyfrowanie jest bardzo cenne dla zabezpieczania danych podczas przesyłania, przetwarzania i przechowywania, ma również wady:

- Cyberprzestępcy mogą je wykorzystać do przejęcia danych osób i organizacji, żądając okupu za przywrócenie dostępu – tzw. atak ransomware.
- Skuteczne zarządzanie kluczami szyfrującymi, tak aby nie zostały skompromitowane, jest trudne, co może umożliwić cyberprzestępcom zdobycie kluczy i naruszenie poufności oraz integralności danych.
- Narastają obawy, że gdy technologie obliczeń kwantowych dojrzeją, będą w stanie złamać zaawansowane schematy szyfrowania, na których obecnie opiera się ochrona danych.

Uwierzytelnianie: mechanizm kontroli dostępu umożliwiający weryfikację, czy użytkownik, urządzenie lub aplikacja jest tym, za kogo się podaje. Dane uwierzytelniające (nazwa użytkownika i hasło) są porównywane z bazą danych uprawnionych użytkowników lub z serwerami uwierzytelniania, co pozwala zweryfikować tożsamość i prawo dostępu do urządzenia, serwerów, aplikacji lub bazy danych. Uwierzytelnianie za pomocą nazwy użytkownika lub identyfikatora i hasła nazywa się uwierzytelnianiem jednoskładnikowym. Obecnie organizacje, zwłaszcza przetwarzające dane wrażliwe (np. banki), wymagają od użytkowników i aplikacji podania wielu składników uwierzytelniania (a nie tylko identyfikatora i hasła), co nazywa się uwierzytelnianiem wieloskładnikowym; w przypadku dwóch składników – dwuskładnikowym. Wykorzystanie cech człowieka, takich jak odcisk palca, skan twarzy lub siatkówki czy rozpoznawanie głosu, nazywa się uwierzytelnianiem biometrycznym [6)].
Uwierzytelnianie chroni poufność i integralność danych i systemów, dopuszczając do cennych i wrażliwych zasobów (np. komputerów, sieci bezprzewodowych, punktów dostępowych, baz danych, stron internetowych oraz innych aplikacji i usług sieciowych) wyłącznie uwierzytelnionych użytkowników, aplikacje i procesy.

Autoryzacja: podobnie jak uwierzytelnianie, autoryzacja służy ochronie danych i systemów informatycznych przed nadużyciami ze strony cyberprzestępców oraz niezamierzonymi (lub zamierzonymi) działaniami uprawnionych użytkowników. Autoryzacja to proces określania praw dostępu użytkowników i aplikacji w celu sprawdzenia, czy mają prawo wykonać daną czynność. W odróżnieniu od uwierzytelniania, które weryfikuje tożsamość i udziela dostępu do systemu, autoryzacja określa uprawnienia do wykonywania konkretnych czynności. Przykładem autoryzacji jest lista kontroli dostępu (ang. *Access Control List*, ACL), która zezwala lub odmawia użytkownikom i aplikacjom dostępu do określonych zasobów systemu oraz wykonywania określonych czynności. Zwykli użytkownicy mogą mieć prawo do niektórych czynności, a do innych nie, natomiast superużytkownicy lub administratorzy mogą wykonywać niemal wszystkie czynności w systemie. Niektórzy użytkownicy mają dostęp do części danych, ale nie do danych bardziej wrażliwych – w systemach bazodanowych zwykli użytkownicy mogą mieć dostęp do danych mniej wrażliwych, a

administrator do bardziej wrażliwych.

Kontrola dostępu: różne mechanizmy zaprojektowane i wdrożone w celu udzielania uprawnionym użytkownikom dostępu do zasobów systemu informatycznego i kontrolowania czynności, jakie mogą wykonywać (np. przeglądanie, modyfikacja, aktualizacja, instalacja, usuwanie). Może również obejmować fizyczny dostęp do krytycznych zasobów organizacji. Kontrola dostępu chroni poufność i integralność danych i systemów. Fizyczna kontrola dostępu dotyczy fizycznego dostępu do krytycznych zasobów, a logiczna – dostępu do systemów informatycznych (sieci, węzłów obliczeniowych, serwerów, plików i baz danych). Dostęp do miejsc przechowywania krytycznych zasobów (serwerów, sprzętu sieciowego, dokumentów) ogranicza się za pomocą elektronicznych systemów kontroli dostępu wykorzystujących klucze, czytniki kart, klawiatury PIN oraz audyty i raporty śledzące wejścia pracowników. Dostęp do systemów informatycznych ogranicza się mechanizmami uwierzytelniania i autoryzacji weryfikującymi dane logowania, którymi mogą być hasła, kody PIN, skany biometryczne, tokeny bezpieczeństwa lub inne składniki uwierzytelniania [7)].

Niezaprzeczalność: sposób zapewnienia, że nadawca danych nie zaprzeczy ich wysłaniu, a odbiorca – ich otrzymaniu. Gwarantuje również, że podmiot, który podpisał dokument, nie może zaprzeczyć swojemu podpisowi. Pojęcie to zaczerpnięto z dziedziny prawa; stało się ono jednym z pięciu filarów zapewniania bezpieczeństwa informacji, obok poufności, integralności, dostępności i uwierzytelniania. Zapewnia autentyczność i integralność wiadomości: potwierdza odbiorcy tożsamość nadawcy, a nadawcy – że wiadomość została dostarczona bez zmian. Dzięki temu ani nadawca, ani odbiorca nie mogą zaprzeczyć wysłaniu, odebraniu lub przetworzeniu danych. Do zapewnienia niezaprzeczalności można stosować podpisy, o ile są unikalne dla każdego podmiotu.

Rozliczalność: rozliczalność wymaga od organizacji podjęcia wszelkich niezbędnych kroków w celu zapobiegania cyberatakom i ograniczania ryzyka ich wystąpienia. Jeśli do ataku dojdzie, organizacja musi wziąć odpowiedzialność za szkody i zaangażować odpowiednich interesariuszy w usuwanie skutków i zapobieganie przyszłym atakom. Musi również przyjąć odpowiedzialność za radzenie sobie z wyzwaniami bezpieczeństwa i konsekwencjami naruszeń.

1)
Stephen J. Bigelow, DataIntegrity, https://www.techtarget.com/searchdatacenter/definition/integrity
2)
Abi Tyas Tunggal, What is Cybersecurity Risk? A Thorough Definition, https://www.upguard.com/blog/cybersecurity-risk, 2024
3)
Rapid 7, Vulnerabilities, Exploits, and Threats, https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/
4)
Cloudflare, What is an attack vector? https://www.cloudflare.com/learning/security/glossary/attack-vector/
5)
Fortinet, What Is An Attack Surface?, https://www.fortinet.com/resources/cyberglossary/attack-surface
6)
Nick Barney, Authentication, https://www.techtarget.com/searchsecurity/definition/authentication
7)
Gavin Wright,What is access control?, https://www.techtarget.com/searchsecurity/definition/access-control

From:
https://dokuwiki.zmitac.aei.polsl.pl/ - **RAU6 Dokuwiki**

Permanent link:
https://dokuwiki.zmitac.aei.polsl.pl/pl:edu:zmitac:kato:bsiir:lectures:cybersecurity_concepts?rev=1793525929

Last update: **2026/11/01 10:38**