Wytyczne dot. cyberbezpieczeństwa dla pracowników podmiotów kolejowych

European Commission
Transport cybersecurity toolkit

Aktorzy zagrożeń

Osoby fizyczne lub organizacje mogą umyślnie lub nieumyślnie ujawniać i wykorzystywać podatności, które mogą potencjalnie powodować incydenty i wpływać na usługi transportowe, w tym na ich bezpieczeństwo, ochronę, działanie, finanse i reputację. Aktorzy zagrożeń to między innymi grupy sponsorowane przez organy państwowe, cyberprzestępcy, cyberterroryści, haktywiści[1], hakerzy (w tym skrypt krakerzy[2]) oraz osoby legalnie posiadające dostęp do wewnętrznych informacji (w tym uprzywilejowane osoby posiadające legalny dostęp do takich informacji).

Najważniejszymi destrukcyjnymi aktorami celowo atakującymi organizacje transportowe są **cyberprzestępcy**, **osoby legalnie posiadające dostęp do wewnętrznych informacji**, państwa narodowe i **grupy sponsorowane przez organy państwowe**. Przeciwnicy, tacy jak cyberprzestępcy, przeprowadzają zmasowane kampanie cyberataków i często starają się uzyskiwać pieniężne profity.

Legalnie posiadający dostęp do wewnętrznych informacji znają specyfikę organizacji, dla których pracują, i często doskonale zdają sobie sprawę z subtelnych luk w zabezpieczeniach. Wewnętrzni aktorzy zagrożeń to między innymi niezadowoleni pracownicy, dostawcy i indywidualni wykonawcy. W miarę wzrostu globalnych napięć geopolitycznych, państwa narodowe i **grupy sponsorowane przez organy państwowe** stawiają sobie długoterminowe cele strategiczne. Często próbują one ukryć się w głębi struktury organizacji i gromadzić wrażliwe informacje. Po zdobyciu przyczółków w systemach cyfrowych, napastnicy sponsorowani przez organy państwowe starają się zająć pozycje, które zagwarantują spowodowanie jak największych szkód. Na przykład, mogą zaatakować systemy innych organizacji, wykorzystując połączenia sieciowe zinfiltrowanej organizacji.

Do aktorów zagrożeń zalicza się także osoby posiadające dostęp do wewnętrznych informacji, które mogą nieumyślnie lub przypadkowo podejmować działania skutkujące zdarzeniami związanymi z cyberbezpieczeństwem, a w najgorszych przypadkach incydentami cybernetycznymi mającymi wpływ na bezpieczeństwo i ochronę usług transportowych.

Pojawiające się cyber-zagrożenia

Istnieje wiele cyber-zagrożeń ukierunkowanych na transport: rozproszone blokowania usług (DDoS), blokowania usługi (DoS), kradzieże danych, rozpowszechnianie złośliwego oprogramowania (malwaru), phishing, manipulacje oprogramowaniem, nieuprawniony dostęp, ataki destrukcyjne, fałszowanie lub obchodzenie procesów decyzyjnych angażujących operatorów cyberbezpieczeństwa, maskarady tożsamości, nadużywanie przywilejów dostępu, inżynieria społeczna, niszczenie wizerunku, podsłuchy, niewłaściwe wykorzystywanie aktywów, czy manipulacje sprzętem.

W oparciu o obszerne badania literaturowe publicznie dostępnych dokumentów oraz wywiady z ekspertami uznano, że do najpilniejszych pojawiających się cyber-zagrożeń mających wpływ na transport należą: złośliwe oprogramowanie (malware), (rozproszone) blokowania usług (DDoS & DoS), nieuprawnione uzyskiwanie dostępu, kradzieże oraz manipulacje oprogramowaniem.

[1] **haktywiści** to osoby, które używają komputerów i sieci do promowania celów społecznych i politycznych, zwłaszcza wolności słowa, praw człowieka i dostępu do informacji,
[2] **skrypt krakerzy** to osoby które używają programów i skryptów napisanych przez innych bez dogłębnej znajomości zasad ich działania, jedynie po to, aby uzyskać nieuprawniony dostęp do komputerowych kont użytkowników lub plików lub żeby przeprowadzać ataki na systemy komputerowe.

Zagrożenie #1: złośliwe oprogramowanie (Malware)

Złośliwe oprogramowanie, które może mieć potencjalny wpływ na osoby lub organizacje w różnych rodzajach transportu.

Zagrożenie #2: (rozproszone) blokowanie usługi ((D)DoS)

Ataki cybernetyczne uniemożliwiające osobom fizycznym lub organizacjom dostęp do odpowiednich usług i zasobów transportowych.

Zagrożenie #3: nieuprawniony dostęp i kradzież

Nieuprawniony dostęp, przywłaszczenie i wykorzystanie krytycznych zasobów.

Zagrożenie #4: manipulacje oprogramowaniem

Ataki cybernetyczne na oprogramowanie w celu zmiany jego działania i przeprowadzania specyficznych ataków.

Zagrożenie #1 złośliwe oprogramowanie (Malware)

Złośliwe oprogramowanie (Malware) obejmuje szkodliwe programy, które mogą obejmować różne rodzaje aplikacji, takie jak wirusy, trojany, robaki, ransomware, cryptocurrency-miners oraz wszelkie aplikacje, które mogą potencjalnie mieć negatywny wpływ na organizacje lub osoby prywatne w różnych rodzajach transportu.

Ograniczanie rozprzestrzeniania się złośliwego oprogramowania przeznaczonego do celowego uszkadzania komputerów, serwerów, klientów, sieci lub wszystkich tych elementów jest jednym z głównych priorytetów cyberbezpieczeństwa we wszystkich rodzajach transportu. Typowy wektor ataku może obejmować wiadomości e-mail typu phishing skierowane do pracowników. Inne wektory ataku mogą obejmować różne i wyrafinowane strategie inżynierii społecznej, takie jak podłączenie klucza USB do wolnego portu (np. w celu naładowania telefonu komórkowego). Klikając hiperłącza w podejrzanych wiadomościach e-mail lub otwierając załączniki z plikami, użytkownik może nieświadomie instalować oprogramowanie lub świadomie narażać usługi i zasoby transportowe na niebezpieczeństwo.

Na przykład, cyberatak ransomware WannaCry dotknął ponad 150 krajów i zainfekował ponad 230 000 systemów. Chodziło o oprogramowanie ransomware, które zwykle rozprzestrzenia się za pośrednictwem wiadomości e-mail typu phishing zawierających złośliwe załączniki lub hiperłącza. Ten rodzaj ataku wykorzystuje socjotechnikę w celu wprowadzenia w błąd użytkowników systemu, aby zainstalowali (lub aktywowali) określone złośliwe oprogramowanie.

Dobre praktyki przeciw złośliwemu oprogramowaniu

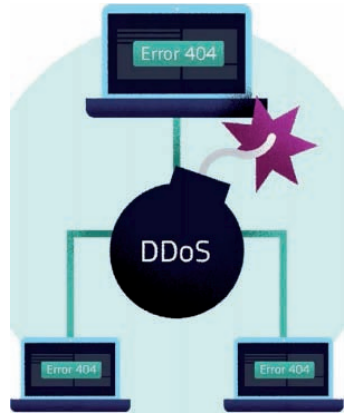
Możesz pomóc w ochronie swojej organizacji, stosując dobre praktyki w zakresie **identyfikacji i zapobiegania rozprzestrzenianiu się złośliwego oprogramowania**, takie jak:

- ❑ **Przestrzeganie zasad bezpieczeństwa**, takich jak skanowanie nośników pamięci i plików w poszukiwaniu wirusów, unikanie otwierania i wysyłania pocztą elektroniczną określonych typów plików (np. plików wykonywalnych, takich jak .exe, .bat .com itp.), instalowanie wyłącznie autoryzowanego oprogramowania, upewnianie się, że oprogramowanie (w tym antywirusowe) jest aktualne i działa prawidłowo, oraz przestrzeganie innych zasad.
- ❑ Regularne **tworzenie kopii zapasowych danych** przy wykorzystaniu bezpiecznych (oraz jednocześnie autoryzowanych) urządzeń lub usług przechowywania danych, które powinny obsługiwać mechanizmy szyfrowania w celu ochrony przechowywanych danych i zapewniać ich dostępność dla procedur przywracania danych.
- ❑ Stosowanie ochrony za pomocą odpowiednich **środków bezpieczeństwa** (np. haseł, szyfrowania itp.) wszystkich systemów, w tym urządzeń mobilnych i urządzeń końcowych, oraz przestrzeganie bezpiecznego zamykania (fizycznego i logicznego) wszystkich systemów, wówczas gdy pozostają bez nadzoru.
- ❑ Unikanie otwierania załączników i klikania hiperłączy zawartych w nieoczekiwanych wiadomościach e-mail i podejrzanych wyskakujących oknach przeglądarek internetowych z dziwnymi tekstami lub pochodzących od nieznanych nadawców oraz z niezaufanych domen internetowych.
- ❑ Unikanie podłączania do komputera **niezaufanych lub nieznanych urządzeń wymiennych**, takich jak pamięci USB, dyski twarde i inne urządzenia pamięci masowej.
- ❑ Unikanie wyłączania zabezpieczeń przed złośliwym oprogramowaniem (np. wyłączania oprogramowania antywirusowego, oprogramowania filtrującego treści, zapór sieciowych itp.)
- ❑ Regularne **aktualizowanie zainstalowanego oprogramowania** do najnowszych dostępnych wersji (które osoby odpowiedzialne za bezpieczeństwo informacji lub administratorzy systemów mogą udostępniać w formie regularnych aktualizacji).
- ❑ Unikanie używania uprzywilejowanych kont (np. na poziomie administratora) i poświadczeń do regularnych działań i eksploatacji.
- ❑ Zgłaszanie osobom odpowiedzialnym za bezpieczeństwo informacji lub administratorom systemów wszelkich podejrzanych wiadomości e-mail lub nieoczekiwanych zachowań systemów.
- ❑ Zwracanie uwagi na bezpieczeństwo informacji w codziennej pracy w celu rozpoznawania problemów związanych z bezpieczeństwem IT i odpowiedniego reagowania.

Zagrożenie #2 (rozproszone) blokowanie usługi

Ataki typu rozproszone blokowanie usługi (DDoS – ang. Distributed Denial of Service) oraz blokowanie usługi (DoS – ang. Denial of Service) wpływają na dostępność i osiągalność danych, usług, systemów i innych zasobów. Tego typu ataki mogą trwać przez różny czas i mogą być skierowane na więcej niż jedną usługę lub system jednocześnie. Ataki DDoS wykorzystują wiele systemów (lub kanałów ataku) w celu przeciążenia docelowych usług lub systemów żądaniami. Udane ataki wpływają na zdolności usług i możliwości systemów w zakresie obsługi niespodziewanej liczby żądań. Skutkuje to blokowaniem dostępu do usług i zasobów.

Należy zauważyć, że dotknięte usługi i systemy należące do organizacji transportowych mogą być wykorzystywane do przeprowadzania ataków DDoS i DoS, których celem są określone systemy eksploatacyjne lub inne organizacje. Zaatakowane mogą zostać na przykład, korporacyjne systemy informacyjne (takie jak komputery osobiste i specjalizowane urządzenia) w celu uzyskania dostępu do technologicznych rozwiązań eksploatacyjnych, które mogą być podłączone do internetu lub do sieci dostępowej w celu przesyłania danych eksploatacyjnych. Połączenia między różnymi systemami i sieciami (takimi jak sieci korporacyjne, technologiczne rozwiązania eksploatacyjne i zdalny dostęp serwisowy) mogą stanowić podatności na ataki DDoS lub DoS na krytyczne usługi i systemy transportowe. Przykładowo, ataki DDoS i DoS mogą wykorzystywać powszechnie stosowane protokoły sieciowe i komunikacyjne, takie jak Web Services Dynamic Discovery (WS Discovery), które urządzenia IoT mogą wykorzystywać do automatycznego wykrywania każdego węzła w sieciach lokalnych (LAN). Jeśli urządzenia IoT posiadają podatności na ataki, osoby atakujące mogą je wykorzystać do wykrycia innych podłączonych urządzeń i przeprowadzenia ataków DDoS lub DoS.



Dobre praktyki przeciw (rozproszonemu) blokowaniu usługi

Możesz pomóc w ochronie swojej organizacji, identyfikując ataki typu **rozproszone blokowanie usługi** (**DDoS**) i **blokowanie usługi** (**DoS**). Należy niezwłocznie skontaktować się z zespołami ds. bezpieczeństwa i zespołami IT w przypadku wykrycia lub doświadczenia któregokolwiek z poniższych wskaźników potencjalnie świadczących o trwającym ataku DDoS i/lub DoS na twoje usługi lub systemy:

- ❑ Wzrost żądań zużywających przepustowość sieci (postrzegany jako powolna realizacja usługi czy długi czas odpowiedzi) powodujący awarie usług lub systemu z powodu przeciążenia.
- ❑ Wzrost zapotrzebowania na korzystanie z zasobów pamięci bez wyraźnej przyczyny.
- ❑ **Nieoczekiwane zachowanie usług i systemów**, częste awarie i dziwne komunikaty o błędach spowodowane destrukcyjnym zużyciem zasobów obliczeniowych lub połączeń sieciowych.
- ❑ **Obniżona wydajność** urządzeń, długi czas wykonywania prostych zadań oraz zauważalne zmiany działania (np. głośno pracujący wentylator przy wolno działających urządzeniach).
- ❑ **Nieoczekiwane połączenia internetowe lub utrata połączeń** z usługami i systemami.
- ❑ Subtelne zmiany w zachowaniu urządzeń sterujących lub technologii, powodujące uszkodzenia fizyczne.
- ❑ Odmowy dostępu do kont uprzywilejowanych lub administracyjnych w celu blokowania odtworzeniowych procedur reagowania na incydenty.

Zagrożenie #3 nieuprawniony dostęp i kradzież

Aktorzy zagrożeń mogą chcieć uzyskać logiczny lub fizyczny dostęp bez zezwolenia do sieci, systemu, aplikacji, danych lub innego zasobu w celu przeprowadzenia destrukcyjnych działań, w tym kradzieży wrażliwych danych lub zasobów (w tym zasobów fizycznych).

Zagrożenia związane z nieuprawnionym dostępem i kradzieżą dotyczą aktywów poufnych i zastrzeżonych (w tym identyfikatorów osobistych, danych uwierzytelniających do kont uprzywilejowanych czy systemów oraz różnego typu poufnych i zastrzeżonych informacji). Zagrożenia te mogą wykorzystywać luki w systemach, jak również nieświadome osoby ujawniające dane wrażliwe, takie jak dane uwierzytelniające (login, hasło itp.) lub dane osobowe (e-mail, osobisty numer identyfikacyjny itp.).

W odniesieniu do nieuprawnionego dostępu kradzież tożsamości polega na bezprawnym wykorzystaniu danych osobowych lub niepowtarzalnych identyfikatorów w celu podszywania się pod osoby lub pod usługi czy systemy, w celu uzyskania dostępu do zasobów prywatnych lub zastrzeżonych (w tym np. zasobów finansowych i fizycznych). Takie cyber-zagrożenia mogą być również skierowane przeciwko aktywom fizycznym we wszystkich rodzajach transportu.

Dobre praktyki przeciw nieuprawnionemu dostępowi i kradzieży

W celu zapobiegania atakom polegającym na nieuprawnionym dostępie i kradzieży, konieczne jest przestrzeganie zasad takich jak „tylko niezbędna wiedza" (ang. „need to know") oraz „domyślnie z ochroną i zapewnieniem prywatności" (ang. „security and privacy by default"), które podkreślają, że wrażliwe i poufne aktywa (w tym dane osobowe i dane wrażliwe oraz dane i aktywa systemów transportowych itp.) powinny być dostępne tylko dla tych, którzy potrzebują praw dostępu w celu wykonywania swoich obowiązków.

Możesz pomóc w ochronie swojej organizacji, stosując dobre praktyki w zakresie identyfikacji i zapobiegania nieuprawnionemu dostępowi i kradzieżom, takie jak:

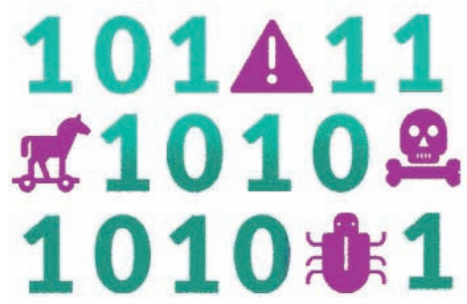
- ❑ Przestrzeganie organizacyjnych polityk dotyczących bezpieczeństwa.
- ❑ Unikanie udostępniania i publikowania danych uwierzytelniających i osobowych online, w tym zdjęć, które mogą zawierać takie informacje.
- ❑ Unikanie używania lub przesyłania do niezaufanych i niezabezpieczonych sieci, urządzeń lub usług internetowych (np. stron internetowych, które używają niezabezpieczonych protokołów lub adresów http://, a nie bezpiecznych adresów https://) danych uwierzytelniających i danych osobowych (oraz innych danych wrażliwych).
- ❑ **Nieujawnianie nigdy i nikomu swoich danych uwierzytelniających** (np. loginu i hasła), nawet przez e-mail lub telefon.
- ❑ Chronienie wrażliwych danych wpisywanych na klawiaturach lub wyświetlanych na ekranach (w tym na urządzeniach mobilnych) przed nieupoważnionymi osobami, korzystanie z ekranów chroniących prywatność (filtrów prywatyzujących), unikanie pracy w miejscach publicznych z prywatnymi urządzeniami oraz unikanie pozostawiania jakichkolwiek urządzeń odblokowanych i bez nadzoru.
- ❑ **Używanie złożonych haseł** (np. wystarczająco długich haseł łączących znaki alfanumeryczne i specjalne) zgodnych z odpowiednią polityką bezpieczeństwa organizacji, aby zapobiec nieuprawnionemu dostępowi.
- ❑ **Zmienianie domyślnych haseł** podłączonych systemów i urządzeń (np. drukarek, routerów, kamer, inteligentnych zamków itp.)
- ❑ Unikanie używania tych samych danych uwierzytelniających (np. loginu i hasła) do wielu usług i systemów oraz unikanie używania tych samych danych uwierzytelniających do usług i systemów, które wymagają kont uprzywilejowanych.
- ❑ Wysyłanie haseł i kluczy do przesyłanych plików chronionych (np. archiwów ZIP) tylko kanałem całkowicie niezależnym (np. wiadomością SMS przez GSM lub rozmową telefoniczną) i nigdy pocztą elektroniczną.
- ❑ Jeśli możliwe, **aktywowanie uwierzytelniania dwuskładnikowego** (2FA) lub wieloskładnikowego (MFA).

Zagrożenie #4 manipulacja oprogramowaniem

Nieprawidłowe konfiguracje i manipulacje oprogramowaniem oraz powiązanymi z nim systemami lub składnikami mogą mieć bezpośredni wpływ na stan bezpieczeństwa usług i systemów transportowych. Ataki cybernetyczne wykorzystujące manipulacje oprogramowaniem modyfikują ustawienia oprogramowania lub wpływają na integralność danych w celu zmiany zachowania systemów i usług.

Atakujący mogą celowo manipulować oprogramowaniem (lub jego częścią) w celu uzyskania korzyści z dostępu do wrażliwych zasobów (np. uzyskania nieuprawnionego dostępu, uniemożliwienia uprawnionym osobom lub systemom dostępu do niezbędnych zasobów, gromadzenia poufnych informacji, wprowadzania zmian w sposobie realizacji funkcji itp.).

Na przykład atakujący mogą celować w kanały komunikacyjne producentów w celu przesyłania destrukcyjnych aktualizacji oprogramowania usług i systemów (w tym technologii eksploatacyjnych) w czasie eksploatacji. Atakujący wykorzystują naruszone poświadczenia autoryzacji, aby uzyskać dostęp do zabezpieczonego interfejsu sieciowego zdalnego serwisu w celu zainstalowania zmanipulowanego oprogramowania i dalszego narażania na utratę bezpieczeństwa innych dostępnych usług i systemów. Następnie instalują zmanipulowane oprogramowanie, które narusza bezpieczeństwo docelowych usług i systemów lub atakują inne podłączone usługi i/lub systemy.



Dobre praktyki przeciw manipulacjom oprogramowaniem

Możesz pomóc w ochronie swojej organizacji poprzez przestrzeganie dobrych praktyk w zakresie identyfikacji i zapobiegania manipulacji oprogramowaniem, takich jak:

- ❑ Unikanie instalowania niewiarygodnego oprogramowania na systemach i urządzeniach (w tym komputerach osobistych, serwerach, urządzeniach peryferyjnych, urządzeniach sieciowych, smartfonach itp.).
- ❑ Instalowanie zawsze oprogramowania i aktualizacji z oficjalnych źródeł i stron internetowych (np. producentów, repozytoriów firmowych itp.).
- ❑ Unikanie pobierania oprogramowania i aplikacji (oraz wszelkich plików) z nielegalnych źródeł.
- ❑ Odinstalowywanie niepotrzebnego lub ostatnio nieużywanego oprogramowania i wyłączanie niepotrzebnych połączeń (np. protokołów i usług sieciowych), w tym dostępu do usług zdalnych (np. usług przechowywania danych w chmurze).
- ❑ Skanowanie wszelkiego oprogramowania i urządzeń pamięci masowej za pomocą niezawodnego i zaktualizowanego programu antywirusowego.
- ❑ Pobieranie bezpiecznego oprogramowania przemysłowego (np. aktualizacji, poprawek, nowych produktów itp.) od zaufanych dostawców, stosując zasadę białej stacji.
- ❑ Aktualizowanie całego zainstalowanego oprogramowania zgodnie z zasadami i praktykami danej organizacji.