**CIS Controls**

**Grupy wdrożeniowe**

Kontrole CIS cieszą się międzynarodowym uznaniem za połączenie wiedzy eksperckiej na temat zagrożeń, technologii biznesowej i opcji obronnych w skuteczny, spójny i prostszy sposób zarządzania programem poprawy bezpieczeństwa organizacji. Według naszych doświadczeń organizacje każdej wielkości i złożoności wciąż potrzebują więcej pomocy, aby rozpocząć i skupić swoją uwagę i zasoby.  
W tym celu, po raz pierwszy spojrzeliśmy w sposób przekrojowy na wszystkie Kontrole CIS i zidentyfikowaliśmy podstawowy zestaw Kontroli Podrzędnych, które organizacje o ograniczonych zasobach i ograniczonej ekspozycji na ryzyko powinny po prostu wykonać. Nazywamy to grupą wdrożeniową I. Zapewniają one skuteczną wartość bezpieczeństwa dzięki technologii i procesom, które są już ogólnie dostępne, zapewniając jednocześnie podstawę bardziej dostosowanych i wyrafinowanych działań, jeśli jest to uzasadnione. Opierając się na Grupie wdrożeniowej I, zidentyfikowaliśmy dodatkowy zestaw kontroli podrzędnych dla organizacji posiadających więcej zasobów i wiedzy, ale także większą ekspozycję na ryzyko. Jest to grupa wdrożeniowa 2. Wreszcie, pozostałe kontrole podrzędne tworzą grupę wdrożeniową 3.

Te grupy wdrożeniowe zapewniają prosty i dostępny sposób pomocy organizacjom różnych klas w skoncentrowaniu swoich ograniczonych zasobów bezpieczeństwa i w dalszym wykorzystywaniu wartości programu Kontrole CIS, społeczności oraz uzupełniających narzędzi i reklam roboczych.

**Jak zacząć**

Kontrole CIS to stosunkowo niewielka liczba ułożonych wg priorytetu, dobrze sprawdzonych i obsługiwanych działań bezpieczeństwa, które organizacje mogą podjąć, aby ocenić i poprawić swój obecny stan bezpieczeństwa. Zmieniają także dyskusję z „Co powinno zrobić moje przedsiębiorstwo?” na „Co powinniśmy robić WSZYSCY?” by poprawić bezpieczeństwo na szeroką skalę

Nie jest to jednak rozwiązanie uniwersalne, zarówno pod względem treści, jak i priorytetu. Nadal musisz rozumieć, co jest kluczowe dla Twojej firmy, danych, systemów, sieci i infrastruktur, i musisz wziąć pod uwagę wrogie działania, które mogą wpłynąć na twoją zdolność do osiągnięcia sukcesu w biznesie lub działaniu. Nawet stosunkowo niewielka liczba Kontroli nie może być wykonywana naraz, więc musisz opracować plan oceny, wdrożenia i zarządzania procesami.

**Ta wersja Kontroli CIS**

Wraz z wydaniem wersji 6 Kontroli CIS (w październiku 2015 r.) wprowadziliśmy środki w celu lepszego zrozumienia potrzeb użytkowników, zebrania bieżących opinii i zrozumienia, w jaki sposób branża bezpieczeństwa obsługuje kontrolę CIS. Wykorzystaliśmy to, aby napędzać rozwój wersji 7, a także wersji 7.1.

Oprócz wspomnianych wcześniej krytycznych założeń obrony cybernetycznej, staraliśmy się, aby każda kontrola CIS była jasna, zwięzła i aktualna. Chociaż nie ma magicznego rozwiązania podczas definiowania kontroli bezpieczeństwa, uważamy, że ta wersja stanowi podstawę znacznie prostszej i łatwiejszej do wdrożenia implementacji, pomiaru i automatyzacji.

W CIS uważnie słuchamy wszystkich twoich opinii i pomysłów na kontrole CIS. W szczególności wielu z was poprosiło o pomoc w ustalaniu priorytetów i wprowadzaniu zmian w CIS Controls dla swojego programu cyberbezpieczeństwa. Ten temat wymagał znacznego przetworzenia i zaowocował omówieniem poniższych grup wdrożeniowych. W rezultacie następujące zasady zostały użyte do przeprowadzenia aktualizacji V7.1.

• Ponowna ocena schematu priorytetów dla kontroli CIS aż do poziomu kontroli podrzędnych, biorąc pod uwagę zmieniający się krajobraz zagrożeń i ograniczenia zasobów;

• Naprawa drobnych literówek i błędów;

• Zwiększenie przejrzystości i czytelności kontroli głównych i pod-kontroli CIS;

• Powstrzymanie się od dodawania lub odejmowania od treści technicznej Kontroli CIS lub pod-kontroli.

Dostarczamy również szczegółowe informacje o zmianach, aby zminimalizować pracę dla firm, które zdecydują się na migrację z wersji 7 do wersji 7.1. Możesz również pomóc, wysyłając swoje opinie i pomysły dotyczące działań związanych z ustalaniem priorytetów lub innych kwestii na adres controlsinfo@cissecurity.org lub dołączając do społeczności CIS WorkBench (<https://workbench.cisecurity.org/communities/71>).

**O Grupach Wdrożeniowych**

Historycznie, kontole CIS wykorzystywały kolejność Kontroli jako środka skupiającego działania cyberbezpieczeństwa organizacji, czego rezultatem był podzbiór pierwszych sześciu Kontroli CIS określanych jako cyber higiena. Jednak wiele praktyk w zestawie kontroli higieny cybernetycznej CIS może być trudnych dla organizacji z ograniczonymi zasobami. Podkreśliło to potrzebę zebrania najlepszych praktyk skoncentrowanych na równoważeniu ograniczeń zasobów i skutecznym ograniczaniu ryzyka. W rezultacie ClS zaleca następujące nowe wytyczne, aby zhierarchizować wykorzystanie kontroli CIS, znanej jako grupy wdrożeniowe kontroli CIS.

Grupy wdrożeniowe Kontroli CIS to samodzielnie oceniane kategorie organizacji oparte na odpowiednich atrybutach cyberbezpieczeństwa. Każda grupa wdrożeniowa identyfikuje podzbiór Kontroli CIS, który społeczność ogólnie oceniła jako rozsądny dla organizacji o podobnym profilu ryzyka i zasobach. Te grupy wdrożeniowe reprezentują poziomy przekrój kontroli CIS dostosowanych do różnych typów przedsiębiorstw. Każda grupa wdrożeniowa opiera się na poprzedniej. W rezultacie grupa 2 obejmuje również grupę 1, a grupa 3 obejmuje wszystkie kontrole podrzędne CIS w grupie 1 i grupie 2. Organizacja o ograniczonych zasobach może być zmuszona do ochrony danych krytycznych, a tym samym do wdrożenia kontroli podrzędnych w wyższym IG. Ostatecznie organizacja wdrażająca kontrole CIS zdefiniowane dla ich grupy 1 zmierza w kierunku należytej staranności, jak opisano w Metodzie Oceny Ryzyka CIS (CIS RAM). CIS RAM to darmowy zasób dostępny pod adresem <https://learn.cisecurity.org/cis-ram>

CIS zaleca organizacjom hierarchizowanie wdrożenia kontroli poprzez stosowanie się do grup wdrożeniowych. Organizacje powinny wdrożyć kontrole podrzędne w grupie 1, a następnie w grupie 2 i na końcu w grupie 3. Kontrole podrzędne znajdujące się w grupie 1, są niezbędne do osiągnięcia sukcesu. Wdrożenie grupy 1 należy uznać za jedną z pierwszych rzeczy, które należy wykonać w ramach programu cyberbezpieczeństwa. CIS odnosi się do grupy 1 nazywając ją „Cyber Higieną” - podstawowe zabezpieczenia, które należy wprowadzić w celu obrony przed zwykłymi atakami. Organizacje zachęca się do klasyfikowania siebie jako należące do jednej z trzech grup wdrożeniowych. Na przykład:

• Rodzinna firma zatrudniająca mniej niż 10 pracowników może zaklasyfikować się jako grupa 1;

• Organizacja regionalna świadcząca jakąś usługę może sklasyfikować się jako grupa 2; lub

• Duża korporacja z tysiącami pracowników może być w grupie 3.

Po ustaleniu klasyfikacji organizacje mogą skupić się na wdrożeniu kontroli podrzędnych CIS znajdujących się w danej grupie. Kryteria, które organizacje wykorzystują do określenia swojej kategorii organizacyjnej, opierają się na cechach opisanych poniżej:

1. **Wrażliwość danych i krytyczność usług oferowanych przez organizację.** Organizacje świadczące usługi, które muszą być dostępne z konkretnego powodu (np. bezpieczeństwo publiczne, infrastruktura krytyczna) lub praca z danymi, które muszą być chronione w ramach dalszego ograniczonego zestawu wymagań (np. ustawodawstwo federalne), muszą wdrożyć bardziej zaawansowane mechanizmy kontroli bezpieczeństwa cybernetycznego niż te organizacje, które tym się nie zajmują.
2. **Oczekiwany poziom wiedzy technicznej prezentowany przez pracowników.** Wiedza i doświadczenie w zakresie bezpieczeństwa cybernetycznego są trudne do uzyskania, ale są niezbędne do wdrożenia wielu szczegółowych środków łagodzących określonych w kontrolach CIS. Wiele kontroli CIS wymaga minimalnych podstawowych kompetencji informatycznych, podczas gdy inne wymagają dogłębnych umiejętności i wiedzy w zakresie cyberbezpieczeństwa w celu pomyślnego wdrożenia.
3. **Zasoby dostępne i dedykowane działaniom związanym z cyberbezpieczeństwem.** Czas, pieniądze i personel są niezbędne, aby wdrożyć wiele najlepszych praktyk zawartych w kontrolach CIS. Przedsiębiorstwa, które mogą przeznaczyć te zasoby na cyberbezpieczeństwo, mogą stworzyć bardziej wyrafinowaną obronę przed dzisiejszymi przeciwnikami. Chociaż dostępne są narzędzia typu open source, które pomagają organizacjom w implementacji, mogą one wiązać się z dodatkowymi kosztami zarządzania i wdrożenia, które należy rozpoznać i wziąć pod uwagę.

Należy pamiętać, że organizacje zachęca się do przeprowadzenia oceny ryzyka przy użyciu metodologii, takiej jak CIS RAM. To poinformuje, które kontrole podrzędne CIS powinny zostać wdrożone dla organizacji. Grupy implementacyjne nie są nieograniczone; mają one na celu dostarczenie przybliżonej miary, którą organizacje mogą wykorzystać do lepszej hierarchizacji działań związanych z bezpieczeństwem cybernetycznym. Poniżej zdefiniowano i opisano każdą grupę.

**Grupa wdrożeniowa 1:**

Organizacja IG1 jest małą i średnią firmą z ograniczoną wiedzą z zakresu IT i bezpieczeństwa cybernetycznego, która może służyć ochronie zasobów informatycznych i personelu. Głównym problemem tych organizacji jest utrzymanie ciągłości działania, ponieważ mają one ograniczoną tolerancję na przestoje. Wrażliwość danych, które starają się chronić, jest niska i dotyczy głównie informacji o pracownikach i danych finansowych. Jednak mogą istnieć małe i średnie organizacje, które są odpowiedzialne za ochronę poufnych danych, a tym samym zostaną zaliczone do wyższej grupy. Pod-kontrole wybrane do IG1 powinny być możliwe do wdrożenia z ograniczoną wiedzą na temat bezpieczeństwa cybernetycznego i mają na celu udaremnienie ogólnych, nieukierunkowanych ataków. Te Pod-kontrole będą również zazwyczaj zaprojektowane do współpracy ze sprzętem i oprogramowaniem typu COTS do małych biur lub biur w domu.

**Grupa wdrożeniowa 2:**

Organizacja IG2 zatrudnia osoby odpowiedzialne za zarządzanie i ochronę infrastruktury IT. Organizacje te obsługują wiele działów o różnych profilach ryzyka w zależności od funkcji i misji. Małe jednostki organizacyjne mogą mieć obowiązek przestrzegania przepisów. Organizacje IG2 często przechowują i przetwarzają poufne informacje o kliencie lub firmie i mogą wytrzymać krótkie przestoje. Głównym problemem jest utrata zaufania publicznego w przypadku naruszenia. Pod-kontrole wybrane dla IG2 pomagają zespołom bezpieczeństwa radzić sobie ze zwiększoną złożonością operacyjną. Niektóre pod-kontrole będą zależeć od technologii klasy korporacyjnej i specjalistycznej wiedzy, aby prawidłowo je zainstalować i skonfigurować.

**Grupa wdrożeniowa 3:**

Organizacja IG3 zatrudnia ekspertów ds. bezpieczeństwa, którzy specjalizują się w różnych aspektach cyberbezpieczeństwa (np. zarządzanie ryzykiem, testy penetracyjne, bezpieczeństwo aplikacji). Systemy i dane IG3 zawierają poufne informacje lub funkcje, które podlegają nadzorowi regulacyjnemu i nadzorowi zgodności. Organizacja IG3 musi zająć się dostępnością usług oraz poufnością i integralnością danych wrażliwych. Udane ataki mogą spowodować poważne szkody dla dobra publicznego. Pod-kontrole wybrane do IG3 muszą znosić ukierunkowane ataki wyrafinowanego przeciwnika i zmniejszyć wpływ ataków zero-day.

Podczas gdy to podejście zapewnia ogólne wytyczne dotyczące ustalania priorytetów w zakresie korzystania z Kontroli CIS, to nie powinno to zastąpić potrzeby zrozumienia własnej pozycji ryzyka organizacyjnego. Organizacje powinny nadal starać się wykonywać własne obowiązki w zakresie analizy opieki i dostosowywać wdrażanie kontroli CIS w oparciu o to, co jest odpowiednie i uzasadnione, biorąc pod uwagę ich zasoby, misję i ryzyko. Korzystając z typu metod opisanych w CIS RAM, organizacje różnych grup wdrożeniowych mogą podejmować decyzje oparte na ryzyku, dotyczące tego, które kontrole podrzędne w ich grupie mogą pominąć a do których wyższych grup powinny dążyć. Chodzi o to, aby pomóc organizacjom skoncentrować wysiłki na dostępnych zasobach i zintegrować je z każdym wcześniejszym procesem zarządzania ryzykiem.

|  |  |  |  |
| --- | --- | --- | --- |
| Definicje | 1 | 2 | 3 |
| Kontrole podrzędne CIS dla środowisk oprogramowania, które są domowe lub małe komercyjne i dostępne w sklepach, w których czułość danych zazwyczaj mieści się w grupie 1. Pamiętaj, że wszelkie kroki grupie 1 powinny być również przestrzegane przez organizacje w grupie 2 i 3. | ✓ | ✓ | ✓ |
| Kontrole podrzędne CIS koncentrujące się na pomocy zespołom bezpieczeństwa w zarządzaniu wrażliwymi informacjami o kliencie lub firmie podlegają grupie 2. Kroki z grupy 2 powinny być również przestrzegane przez organizacje w G3. |  | ✓ | ✓ |
| Kontrole podrzędne CIS, które zmniejszają wpływ ataków zero-day i ukierunkowanych ataków wyrafinowanych przeciwników, zazwyczaj należą do grupy 3. Organizacje z grupy 1 i 2 mogą nie być w stanie wdrożyć kontroli podrzędnych grupy 3. |  |  | ✓ |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Kontrola CIS** | **Kontrola podrzędna CIS** | **Rodzaj zasobu** | **Funkcja bezpieczeństwa** | **Tytuł** | **Opis** | **IG 1** | **IG 2** | **IG 3** |
| **1** | | | | **Spis i kontrola zasobów sprzętowych**  ***Aktywnie zarządzaj (prowadź spis, śledź i koryguj) wszystkie urządzenia sprzętowe w sieci, tak aby dostęp do nich miały tylko autoryzowane urządzenia, a nieautoryzowane i niezarządzane urządzenia zostały znalezione i uniemożliwiono im dostęp.*** | |  | | |
|
| 1 | 1.1 | Urządzenia | Identyfikacja | Wykorzystaj narzędzie Active Discovery | Wykorzystaj narzędzie Active discovery, aby zidentyfikować urządzenia podłączone w organizacji do sieci i zaktualizować spis zasobów sprzętowych. |  | X | X |
| 1 | 1.2 | Urządzenia | Identyfikacja | Wykorzystaj narzędzie do pasywnego wykrywania zasobów | Wykorzystaj narzędzie do pasywnego wykrywania, aby zidentyfikować urządzenia podłączone do sieci organizacji i automatycznie aktualizować spis zasobów sprzętowych. |  |  | X |
| 1 | 1.3 | Urządzenia | Identyfikacja | Użyj rejestrowania DHCP, aby zaktualizować spis zasobów | Użyj DHCP (Dynamic Host Configuration Protocol) na wszystkich serwerach DHCP lub narzędziach zarządzania adresami IP, aby zaktualizować spis zasobów sprzętowych organizacji. |  | X | X |
| 1 | 1.4 | Urządzenia | Identyfikacja | Utrzymuj szczegółowy spis zasobów | Utrzymuj dokładny i aktualny spis wszystkich zasobów technologicznych z możliwością przechowywania lub przetwarzania informacji. Spis ten powinien obejmować wszystkie zasoby sprzętowe, niezależnie od tego, czy są podłączone do sieci organizacji czy nie. | X | X | X |
| 1 | 1.5 | Urządzenia | Identyfikacja | Zachowaj informacje o spisie zasobów | Upewnij się, że spis zasobów sprzętowych rejestruje adres sieciowy, adres sprzętowy, nazwę komputera, właściciela zasobu danych i dział dla każdego zasobu oraz czy zasób sprzętowy został zatwierdzony do połączenia z siecią. |  | X | X |
| 1 | 1.6 | Urządzenia | Odpowiedź | Znajdź nieautoryzowane zasoby | Upewnij się, że nieautoryzowane zasoby są usuwane z sieci, poddawane kwarantannie lub magazyn jest aktualizowany w odpowiednim czasie. | X | X | X |
| 1 | 1.7 | Urządzenia | Ochrona | Wdróż kontrolę dostępu na poziomie portu | Wykorzystaj kontrolę dostępu na poziomie portu, zgodnie ze standardami 802.1x, do kontrolowania, które urządzenia mogą uwierzytelniać się w sieci. System uwierzytelniania należy powiązać z spisem zasobu danych sprzętowych, aby upewnić się, że tylko autoryzowane urządzenia mogą łączyć się z siecią. |  | X | X |
| 1 | 1.8 | Urządzenia | Ochrona | Wykorzystaj certyfikaty klienta do uwierzytelniania zasobów sprzętowych | Użyj certyfikatów klienta do uwierzytelniania zasobów sprzętowych łączących się z zaufaną siecią organizacji. |  |  | X |
| **2** | | | | **Spis i kontrola oprogramowania**  ***Aktywnie zarządzaj (prowadź spis, śledź i koryguj)* całe oprogramowanie w sieci, dzięki czemu tylko autoryzowane oprogramowanie będzie instalowane i uruchamiane oraz że nieautoryzowane i niezarządzane oprogramowanie zostanie znalezione i instalacja lub uruchomienie zostanie uniemożliwione.** | |  | | |
|
| 2 | 2.1 | Aplikacje | Identyfikacja | Prowadź spis autoryzowanego oprogramowania | Prowadź aktualną listę wszystkich autoryzowanych programów, które są wymagane w przedsiębiorstwie do wszelkich celów biznesowych w dowolnym systemie biznesowym. | X | X | X |
| 2 | 2.2 | Aplikacje | Identyfikacja | Upewnij się, że oprogramowanie jest wspierane przez dostawcę | Upewnij się, że tylko autoryzowane aplikacje lub systemy operacyjne są dodawane do spisu autoryzowanego oprogramowania organizacji oraz że są regularnie uaktualniane przez producenta. Niewspierane oprogramowanie należy oznaczyć jako “unsupported” w spisie. | X | X | X |
| 2 | 2.3 | Aplikacje | Identyfikacja | Wykorzystaj narzędzia do inwentaryzacji oprogramowania | Wykorzystaj narzędzia do inwentaryzacji oprogramowania w całej organizacji, aby zautomatyzować dokumentację całego oprogramowania w systemach biznesowych. |  | X | X |
| 2 | 2.4 | Aplikacje | Identyfikacja | Śledź informacje o oprogramowaniu | System inwentaryzacji oprogramowania powinien śledzić nazwę, wersję, wydawcę i datę instalacji całego oprogramowania, w tym systemów operacyjnych autoryzowanych przez organizację. |  | X | X |
| 2 | 2.5 | Aplikacje | Identyfikacja | Zintegruj spisy zasobów oprogramowania i sprzętu | System inwentaryzacji oprogramowania powinien być powiązany z spisem zasobów sprzętowych, aby wszystkie urządzenia i powiązane oprogramowanie były śledzone z jednej lokalizacji. |  |  | X |
| 2 | 2.6 | Aplikacje | Odpowiedź | Znajdź niezatwierdzone oprogramowanie | Upewnij się, czy nieautoryzowane oprogramowanie zostało usunięte lub spis jest aktualizowany w odpowiednim czasie | X | X | X |
| 2 | 2.7 | Aplikacje | Ochrona | Wykorzystaj technologię białej listy aplikacji | Wykorzystaj technologię białej listy aplikacji na wszystkich zasobach, aby zagwarantować, że tylko autoryzowane oprogramowanie zostanie uruchomione, a wszelkie nieautoryzowane oprogramowanie zostanie zablokowane. |  |  | X |
| 2 | 2.8 | Aplikacje | Ochrona | Wdróż białą listę dla biblotek | Oprogramowanie białej listy aplikacji musi upewniać się, że tylko autoryzowane biblioteki oprogramowania (takie jak \*.dll, \*.ocx, \*.so itp.) mogą być wczytywane do procesu systemowego. |  |  | X |
| 2 | 2.9 | Aplikacje | Ochrona | Wdróż białą listę dla skryptów | Oprogramowanie białej listy aplikacji musi upewniać się, że tylko autoryzowane i podpisane cyfrowo skrypty (takie jak \*.ps1, \*.py, makra itp.) mogą działać w systemie. |  |  | X |
| 2 | 2.10 | Aplikacje | Ochrona | Fizycznie lub logicznie segreguj aplikacje wysokiego ryzyka | Systemy izolowane fizycznie lub logicznie powinny być wykorzystywane do izolowania i uruchamiania oprogramowania, które jest wymagane do prowadzenia działalności gospodarczej, ale wiąże się z większym ryzykiem dla organizacji. |  |  | X |
| **3** | | | | **Ciągłe zarządzanie podatnością**  ***Ciągle zdobywaj, oceniaj i podejmuj działania w związku z nowymi informacjami w celu identyfikacji słabych punktów, zaradzenia i zminimalizowania szansy dla atakujących.*** | |  | | |
|
| 3 | 3.1 | Aplikacje | Wykrywanie | Używaj zautomatyzowanych narzędzi do skanowania podatności | Wykorzystaj aktualne narzędzie do skanowania luk w zabezpieczeniach SCAP (Security Content Automation Protocol), aby automatycznie skanować wszystkie systemy w sieci co tydzień lub częściej, aby zidentyfikować wszystkie potencjalne luki w systemach organizacji. |  | X | X |
| 3 | 3.2 | Aplikacje | Wykrywanie | Wykonaj uwierzytelnione skanowanie podatności | Wykonaj uwierzytelnione skanowanie luk za pomocą agentów działających lokalnie w każdym systemie lub za pomocą skanerów zdalnych skonfigurowanych z podwyższonymi uprawnieniami do testowanego systemu. |  | X | X |
| 3 | 3.3 | Użytkownicy | Ochrona | Chroń dedykowane konta oceny | Użyj dedykowanego konta do uwierzytelnionych skanowań podatności, które nie powinno być używane do żadnych innych czynności administracyjnych i powinno być powiązane z określonymi komputerami na określonych adresach IP. |  | X | X |
| 3 | 3.4 | Aplikacje | Ochrona | Wdróż narzędzia do automatycznego zarządzania poprawkami systemu operacyjnego | Wdrażaj zautomatyzowane narzędzia do aktualizacji oprogramowania, aby upewnić się, że systemy operacyjne korzystają z najnowszych aktualizacji zabezpieczeń dostarczonych przez dostawcę oprogramowania. | X | X | X |
| 3 | 3.5 | Aplikacje | Ochrona | Wdrażaj zautomatyzowane narzędzia do zarządzania poprawkami oprogramowania | Wdrażaj zautomatyzowane narzędzia do aktualizacji oprogramowania, aby zapewnić, że oprogramowanie firm zewnętrznych we wszystkich systemach pracuje na najnowszych aktualizacjach zabezpieczeń dostarczonych przez dostawcę oprogramowania. | X | X | X |
| 3 | 3.6 | Aplikacje | Odpowiedź | Porównaj skanowanie luk w zabezpieczeniach | Regularnie porównuj wyniki kolejnych skanów podatności, aby sprawdzić, czy luki zostały naprawione w odpowiednim czasie. |  | X | X |
| 3 | 3.7 | Aplikacje | Odpowiedź | Wykorzystaj proces oceny ryzyka | Wykorzystaj proces oceny ryzyka, aby nadać priorytet naprawie wykrytych luk. |  | X | X |
| **4** | | | | **Kontrolowane użycie przywilejów administracyjnych**  ***Procesy i narzędzia używane do śledzenia / kontroli / zapobiegania / poprawiania użycia, przypisania i konfiguracji uprawnień administracyjnych na komputerach, sieciach i aplikacjach.*** | |  | | |
|
| 4 | 4.1 | Użytkownicy | Wykrywanie | Prowadź spis kont admnistracyjnych | Korzystaj z automatycznych narzędzi do inwentaryzacji wszystkich kont administracyjnych, w tym kont domenowych i lokalnych, aby zapewnić, że tylko upoważnione osoby mają podwyższone uprawnienia. |  | X | X |
| 4 | 4.2 | Użytkownicy | Ochrona | Zmień domyślne hasła | Przed wdrożeniem nowego zasobu zmień wszystkie domyślne hasła, aby wartości były zgodne z kontami na poziomie administracyjnym. | X | X | X |
| 4 | 4.3 | Użytkownicy | Ochrona | Zapewnij korzystanie z dedykowanych kont administracyjnych | Upewnij się, że wszyscy użytkownicy posiadający dostęp do konta administracyjnego korzystają z dedykowanego lub dodatkowego konta do podwyższonej aktywności. To konto powinno być używane tylko do czynności administracyjnych, a nie do przeglądania Internetu, poczty e-mail lub podobnych działań. | X | X | X |
| 4 | 4.4 | Użytkownicy | Ochrona | Używaj unikalnych haseł | Tam, gdzie uwierzytelnianie wieloczynnikowe nie jest obsługiwane (takie jak konta administratora lokalnego, konta root lub konta usług), konta będą używać unikalnych haseł dla tego systemu. |  | X | X |
| 4 | 4.5 | Użytkownicy | Ochrona | Użyj uwierzytelniania wieloczynnikowego dla całego dostępu administracyjnego | Użyj uwierzytelniania wieloczynnikowego i kanałów zaszyfrowanych dla całego dostępu do konta administracyjnego. |  | X | X |
| 4 | 4.6 | Użytkownicy | Ochrona | Użyj dedykowanych stacji roboczych do wszystkich zadań administracyjnych | Upewnij się, że administratorzy używają dedykowanego komputera do wszystkich zadań administracyjnych lub zadań wymagających dostępu administracyjnego. Ta maszyna zostanie oddzielona od głównej sieci organizacji i nie będzie miała dostępu do Internetu. Ta maszyna nie będzie używana do czytania wiadomości e-mail, tworzenia dokumentów ani przeglądania Internetu. |  | X | X |
| 4 | 4.7 | Użytkownicy | Ochrona | Ogranicz dostęp do narzędzi skryptowych | Ogranicz dostęp do narzędzi skryptowych (takich jak Microsoft® PowerShell i Python) tylko użytkownikom administracyjnym lub programistom, którzy potrzebują dostępu do tych funkcji. |  | X | X |
| 4 | 4.8 | Użytkownicy | Wykrywanie | Rejestruj i powiadamiaj o zmianach w członkostwie grupy administracyjnej | Skonfiguruj systemy do rejestrowania i alarmowania, gdy konto zostanie dodane lub usunięte z dowolnej grupy z przypisanymi uprawnieniami administracyjnymi. |  | X | X |
| 4 | 4.9 | Użytkownicy | Wykrywanie | Rejestruj i powiadamiaj o nieudanym logowaniu do konta administracyjnego | Skonfiguruj systemy, aby tworzyły log i alerty o nieudanych logowaniach do konta administracyjnego. |  | X | X |
| **5** | | | | **Bezpieczna konfiguracja sprzętu i oprogramowania na urządzeniach mobilnych, laptopach, stacjach roboczych i serwerach**  ***Ustanowienie, wdrożenie i aktywne zarządzanie (śledzenie, raportowanie, poprawianie) konfiguracji zabezpieczeń urządzeń mobilnych, laptopów, serwerów i stacji roboczych przy użyciu rygorystycznego procesu zarządzania konfiguracją i kontrolą zmian, aby uniemożliwić atakującym wykorzystanie podatnych usług i ustawień.*** | |  | | |
|
| 5 | 5.1 | Aplikacje | Ochrona | Ustal bezpieczne konfiguracje | Zachowaj udokumentowane standardy konfiguracji zabezpieczeń dla wszystkich autoryzowanych systemów operacyjnych i oprogramowania. | X | X | X |
| 5 | 5.2 | Aplikacje | Ochrona | Zachowaj bezpieczne obrazy | Zachowuj bezpieczne obrazy lub szablony dla wszystkich systemów w przedsiębiorstwie w oparciu o zatwierdzone standardy konfiguracji w organizacji. Każde nowe wdrożenie systemu lub istniejący system, który zostanie naruszony, należy zobrazować przy użyciu jednego z tych obrazów lub szablonów. |  | X | X |
| 5 | 5.3 | Aplikacje | Ochrona | Bezpieczne przechowuj obrazy główne | Przechowuj obrazy główne i szablony na bezpiecznie skonfigurowanych serwerach, zatwierdzonych za pomocą narzędzi do monitorowania integralności, aby zapewnić, że możliwe są tylko autoryzowane zmiany obrazów. |  | X | X |
| 5 | 5.4 | Aplikacje | Ochrona | Wdróż narzędzia do zarządzania konfiguracją systemu | Wdrażaj narzędzia do zarządzania konfiguracją systemu, które automatycznie wymuszają i ponownie wdrażają ustawienia konfiguracji do systemów w regularnych odstępach czasu. |  | X | X |
| 5 | 5.5 | Aplikacje | Wykrywanie | Wdróż zautomatyzowane systemy monitorowania konfiguracji | Korzystaj z systemu monitorowania konfiguracji zgodnego z protokołem SCAP (Security Content Automation Protocol), aby zweryfikować wszystkie elementy konfiguracji zabezpieczeń, wyjątki zatwierdzone przez katalog i ostrzec o wystąpieniu nieautoryzowanych zmian. |  | X | X |
| **6** | | | | **Konserwacja, Monitoring, i Analiza logów Audytu**  ***Zbieraj, zarządzaj i analizuj logi audytów wydarzń które mogą pomóc wykryć, zrozumieć, lub powrócić do stanu sprzed ataku*** | |  | | |
|
| 6 | 6.1 | Sieć | Wykrywanie | Wykorzystaj trzy zsynchronizowane źródła czasu | Użyj co najmniej trzech zsynchronizowanych źródeł czasu, z których wszystkie serwery i urządzenia sieciowe regularnie pobierają informacje o czasie, tak aby znaczniki czasu w dziennikach były spójne. |  | X | X |
| 6 | 6.2 | Sieć | Wykrywanie | Aktywuj rejestrowania audytu | Upewnij się, że lokalne rejestrowanie zostało włączone na wszystkich systemach i urządzeniach sieciowych. | X | X | X |
| 6 | 6.3 | Sieć | Wykrywanie | Włącz szczegółowe rejestrowanie | Włącz rejestrowanie systemu, aby zawierało szczegółowe informacje, takie jak źródło zdarzenia, data, użytkownik, znacznik czasu, adresy źródłowe, adresy docelowe i inne przydatne elementy. |  | X | X |
| 6 | 6.4 | Sieć | Wykrywanie | Zapewnij odpowiednie przechowywanie logów | Upewnij się, że wszystkie systemy przechowujące logi mają wystarczającą ilość miejsca na wygenerowane logi. |  | X | X |
| 6 | 6.5 | Sieć | Wykrywanie | Centralne zarządzanie logami | Upewnij się, że odpowiednie logi są agregowane do centralnego systemu zarządzania logami w celu analizy i przeglądu. |  | X | X |
| 6 | 6.6 | Sieć | Wykrywanie | Wdrażaj SIEM lub Log Analytic Tools | Wdrażaj zarządzanie informacjami o bezpieczeństwie i zdarzeniach (SIEM) lub narzędzie analityczne do korelacji i analizy logów. |  | X | X |
| 6 | 6.7 | Sieć | Wykrywanie | Regularnie przeglądaj logi | Regularnie przeglądaj logi, aby zidentyfikować anomalie lub nietypowe zdarzenia. |  | X | X |
| 6 | 6.8 | Sieć | Wykrywanie | Regularnie dostosowuj SIEM | Regularnie dostosowuj swój system SIEM, aby lepiej identyfikować zdarzenia, wobec których można podjąć działania, i zmniejszaj hałas wydarzeń (event noise). |  |  | X |
| **7** | | | | ***Z*abezpieczenia poczty e-mail i przeglądarki internetowej**  ***Zminimalizuj powierzchnię ataku i możliwości atakujących do manipulowania ludzkim zachowaniem poprzez interakcję z przeglądarkami internetowymi i systemami pocztowymi.*** | |  | | |
|
| 7 | 7.1 | Aplikacje | Ochrona | Upewnij się o użyciu w pełni wspieranych przeglądarek i klientów poczty e-mail | Upewnij się, że tylko w pełni wspierane przeglądarki i klienci poczty e-mail mogą być uruchamiane w organizacji, najlepiej tylko w najnowszej wersji przeglądarki i klientów poczty e-mail dostarczonych przez dostawcę. | X | X | X |
| 7 | 7.2 | Aplikacje | Ochrona | Wyłącz niepotrzebne lub nieautoryzowane wtyczki przeglądarki lub klienta poczty e-mail | Odinstaluj lub wyłącz wszelkie nieautoryzowane wtyczki przeglądarki lub klienta poczty e-mail lub add-on’y. |  | X | X |
| 7 | 7.3 | Aplikacje | Ochrona | Ogranicz używanie języków skryptowych w przeglądarkach internetowych i klientach poczty | Upewnij się, że tylko autoryzowane języki skryptowe mogą działać we wszystkich przeglądarkach internetowych i klientach poczty e-mail. |  | X | X |
| 7 | 7.4 | Sieć | Ochrona | Utrzymuj i wymuszaj filtry URL oparte na sieci | Wymuszaj sieciowe filtry URL, które ograniczają zdolność systemu do łączenia się z witrynami niezatwierdzonymi przez organizację. To filtrowanie będzie egzekwowane dla każdego z systemów organizacji, niezależnie od tego, czy są fizycznie w obiektach organizacji czy też nie. |  | X | X |
| 7 | 7.5 | Sieć | Ochrona | Zasubskrybuj usługi kategoryzacji URL | Zasubskrybuj usługi kategoryzacji URL, aby mieć pewność, że są aktualne z najnowszymi dostępnymi definicjami kategorii witryn. Strony bez kategorii są domyślnie blokowane. |  | X | X |
| 7 | 7.6 | Sieć | Wykrywanie | Rejestruj wszystkie żądania URL | Rejestruj wszystkie żądania URL z każdego z systemów organizacji, zarówno on-site, jak i na urządzeniu mobilnym, w celu zidentyfikowania potencjalnie szkodliwej aktywności i wsparcia programów obsługi incydentów w identyfikacji potencjalnie zagrożonych systemów. |  | X | X |
| 7 | 7.7 | Sieć | Ochrona | Użyj usług filtrowania DNS | Użyj usług filtrowania DNS (Domain Name System), aby pomóc zablokować dostęp do znanych szkodliwych domen. | X | X | X |
| 7 | 7.8 | Sieć | Ochrona | Zaimplementuj DMARC i włącz weryfikację po stronie odbiorcy | Aby zmniejszyć prawdopodobieństwo sfałszowanych lub zmodyfikowanych wiadomości e-mail z ważnych domen, należy wdrożyć zasady i weryfikację opartą na domenie uwierzytelniania wiadomości, raportowania i zgodności (DMARC), zaczynając od implementacji Sender Policy Framework (SPF) i standardów DomainKeys Identified Mail (DKIM). |  | X | X |
| 7 | 7.9 | Sieć | Ochrona | Blokuj niepotrzebne typy plików | Zablokuj wszystkie załączniki e-mail wchodzące do bramki e-mail organizacji, jeśli typy plików nie są konieczne dla działalności organizacji. |  | X | X |
| 7 | 7.10 | Sieć | Ochrona | Testuj wszystkie załączniki mailowe | Użyj sandboxingu do analizowania i blokowania przychodzących załączników mailowych ze złośliwym zachowaniem. |  |  | X |
| **8** | | | | **Obrona przed złośliwym oprogramowaniem**  ***Kontroluj instalację, rozprzestrzenianie i wykonywanie szkodliwego kodu w wielu punktach przedsiębiorstwa, optymalizując wykorzystanie automatyzacji, aby umożliwić szybką aktualizację obrony, gromadzenie danych i działania naprawcze.*** | |  | | |
|
| 8 | 8.1 | Urządzenia | Ochrona | Wykorzystaj oprogramowanie do centralnego zarządzania oprogramowaniem antywirusowym | Wykorzystuj centralnie zarządzane oprogramowanie antywirusowe, aby stale monitorować i chronić każdą stację roboczą i serwery organizacji. |  | X | X |
| 8 | 8.2 | Urządzenia | Ochrona | Upewnij się, że oprogramowanie antywirusowe i podpisy są aktualizowane | Upewnij się, że oprogramowanie antywirusowe firmy regularnie aktualizuje swój silnik skanowania i bazę sygnatur. | X | X | X |
| 8 | 8.3 | Urządzenia | Ochrona | Włącz/ wdrażaj systemowe technologie chroniące przed exploitami | Włącz funkcje antyexpliotowe, takie jak DEP lub ASLR, które są dostępne w systemie operacyjnym, lub wdrażaj odpowiednie zestawy narzędzi, które można skonfigurować w celu zastosowania ochrony do szerszego zestawu aplikacji i plików wykonywalnych. |  | X | X |
| 8 | 8.4 | Urządzenia | Wykrywanie | Skonfiguruj skanowanie antywirusowe urządzeń wymiennych | Skonfiguruj urządzenia tak, aby automatycznie przeprowadzały skanowanie nośników wymiennych po złośliwym oprogramowaniu po włożeniu lub podłączeniu. | X | X | X |
| 8 | 8.5 | Urządzenia | Ochrona | Skonfiguruj urządzenia, aby nie uruchamiały automatycznie treści | Skonfiguruj urządzenia, aby nie uruchamiały automatycznie treści z nośników wymiennych. | X | X | X |
| 8 | 8.6 | Urządzenia | Wykrywanie | Scentralizuj rejestrowanie szkodliwego oprogramowania | Wysyłaj wszystkie zdarzenia wykrycia złośliwego oprogramowania do korporacyjnych narzędzi do zarządzania oprogramowaniem antywirusowym i serwerów logów zdarzeń w celu analizy i alarmowania. |  | X | X |
| 8 | 8.7 | Sieć | Wykrywanie | Włącz rejestrowanie zapytań DNS | Włącz rejestrowanie zapytań DNS, aby wykryć wyszukiwanie nazw hostów dla znanych szkodliwych domen. |  | X | X |
| 8 | 8.8 | Urządzenia | Wykrywanie | Włącz rejestrowanie kontroli wiersza poleceń | Włącz rejestrowanie kontroli wiersza poleceń dla command shell, takich jak Microsoft PowerShell i Bash. |  | X | X |
| **9** | | | | **Ograniczenie i kontrola portów sieciowych, protokołów i usług**  ***Zarządzaj (śledź /kontroluj /poprawiaj) bieżącym operacyjnym wykorzystaniem portów, protokołów i usług na urządzeniach sieciowych, aby zminimalizować liczbę luk w zabezpieczeniach dostępnych dla atakujących.*** | |  | | |
|
| 9 | 9.1 | Urządzenia | Identyfikacja | Powiąż aktywne porty, usługi i protokoły z zasobami sprzętowymi w spisie zasobów. | Powiąż aktywne porty, usługi i protokoły z zasobami sprzętowymi w spisie zasobów. |  | X | X |
| 9 | 9.2 | Urządzenia | Ochrona | Upewnij się, że działają tylko zatwierdzone porty, protokoły i usługi | Upewnij się, że działają tylko porty sieciowe, protokoły i usługi nasłuchujące na systemie ze sprawdzonymi potrzebami biznesowymi. |  | X | X |
| 9 | 9.3 | Urządzenia | Wykrywanie | Regularnie przeprowadzaj automatyczne skanowanie portów | Regularnie przeprowadzaj automatyczne skanowanie portów we wszystkich systemach i ostrzegaj, jeśli w systemie wykryte zostaną nieautoryzowane porty. |  | X | X |
| 9 | 9.4 | Urządzenia | Ochrona | Zastosuj zapory po stronie hosta lub filtrowanie portów | Zastosuj zapory po stronie hosta lub narzędzia do filtrowania portów w systemach końcowych, stosując regułę domyślnej odmowy, która powoduje wyłączenie całego ruchu z wyjątkiem jawnie dozwolonych usług i portów. | X | X | X |
| 9 | 9.5 | Urządzenia | Ochrona | Wdróż zapory aplikacji | Umieść zapory aplikacji przed wszystkimi krytycznymi serwerami, aby zweryfikować i walidować ruch przychodzący na serwer. Wszelkie nieautoryzowane ruchy powinny być blokowane i rejestrowane. |  |  | X |
| **10** | | | | **Możliwości odzyskiwania danych**  ***Procesy i narzędzia wykorzystywane do prawidłowego tworzenia kopii zapasowych kluczowych informacji za pomocą sprawdzonej metodologii umożliwiającej szybkie ich odzyskanie.*** | |  | | |
|
| 10 | 10.1 | Dane | Ochrona | Zapewnij regularne automatyczne backupy | Upewnij się, że kopie wszystkich danych systemowych są automatycznie tworzone na bieżąco. | X | X | X |
| 10 | 10.2 | Dane | Ochrona | Wykonaj pełne kopie zapasowe systemu | Upewnij się, że utworzono kopie wszystkich kluczowych systemów organizacji poprzez procesy takie jak obrazowanie, aby umożliwić szybkie odzyskanie całego systemu. | X | X | X |
| 10 | 10.3 | Dane | Ochrona | Przetestuj dane w Backup Media |  |  | X | X |
| 10 | 10.4 | Dane | Ochrona | Chroń backupy | Upewnij się, że kopie zapasowe są odpowiednio chronione za pomocą zabezpieczeń fizycznych lub szyfrowania podczas przechowywania, a także gdy są przenoszone przez sieć. Obejmuje to zdalne tworzenie kopii zapasowych i usługi w chmurze. | X | X | X |
| 10 | 10.5 | Dane | Ochrona | Upewnij się, że wszystkie kopie zapasowe mają co najmniej jedno miejsce docelowe, które jest offline | Upewnij się, że wszystkie kopie zapasowe mają co najmniej jedno miejsce docelowe, które jest offline (tj. niedostępne przez połączenie sieciowe). | X | X | X |
| **11** | | | | **Zabezpiecz konfigurację urządzeń sieciowych, takich jak zapory, routery i przełączniki**  ***Stwórz, wdróż i aktywnie zarządzaj (śledzenie, raportowanie, poprawianie) konfiguracją zabezpieczeń urządzeń infrastruktury sieciowej przy użyciu rygorystycznego procesu zarządzania konfiguracją i kontroli zmian, aby uniemożliwić napastnikom wykorzystanie podatnych usług i ustawień.*** | |  | | |
|
| 11 | 11.1 | Sieć | Identyfikacja | Podtrzymuj standardy konfiguracji zabezpieczeń dla urządzeń sieciowych. | Podtrzymuj udokumentowane standardy konfiguracji zabezpieczeń dla wszystkich autoryzowanych urządzeń sieciowych. |  | X | X |
| 11 | 11.2 | Sieć | Identyfikacja | Prowadź dokumentację reguł ruchu konfiguracji | Wszystkie reguły konfiguracji, które zezwalają na przepływ ruchu przez urządzenia sieciowe, powinny być udokumentowane w systemie zarządzania konfiguracją z podanym powodem biznesowym dla każdej reguły, nazwą konkretnej osoby odpowiedzialnej za ten powód biznesowy i oczekiwanym czasem jego trwania. |  | X | X |
| 11 | 11.3 | Sieć | Wykrywanie | Użyj automatycznych narzędzi do weryfikacji standardowych konfiguracji urządzeń i wykrywania zmian | Porównaj wszystkie konfiguracje urządzeń sieciowych z zatwierdzonymi konfiguracjami zabezpieczeń zdefiniowanymi dla każdego używanego urządzenia sieciowego i ostrzegaj, gdy wykryte zostaną jakiekolwiek odchylenia. |  | X | X |
| 11 | 11.4 | Sieć | Ochrona | Zainstaluj najnowszą wersję wszelkich aktualizacji związanych z zabezpieczeniami na wszystkich urządzeniach sieciowych. | Zainstaluj najnowszą stabilną wersję wszelkich aktualizacji związanych z zabezpieczeniami na wszystkich urządzeniach sieciowych. | X | X | X |
| 11 | 11.5 | Sieć | Ochrona | Zarządzaj urządzeniami sieciowymi za pomocą uwierzytelniania wieloczynnikowego i sesji szyfrowanych. | Zarządzaj wszystkimi urządzeniami sieciowymi za pomocą uwierzytelniania wieloczynnikowego i sesji szyfrowanych. |  | X | X |
| 11 | 11.6 | Sieć | Ochrona | Użyj dedykowanych maszyn do wszystkich zadań administracyjnych sieci | Upewnij się, że inżynierowie sieci używają dedykowanego urządzenia do wszystkich zadań administracyjnych lub zadań wymagających zwiększonego dostępu. Ta maszyna będzie odseparowana od głównej sieci organizacji i nie będzie miała dostępu do Internetu. To urządzenie nie może być używane do czytania wiadomości e-mail, tworzenia dokumentów ani przeglądania Internetu. |  | X | X |
| 11 | 11.7 | Sieć | Ochrona | Zarządzaj infrastrukturą sieciową za pośrednictwem sieci dedykowanej | Zarządzaj infrastrukturą sieciową poprzez połączenia sieciowe, które są oddzielone od biznesowych zastosowań tej sieci, opierając się na oddzielnych sieciach VLAN lub na zupełnie innej fizycznej łączności dla sesji zarządzania urządzeniami sieciowymi. |  | X | X |
| **12** | | | | **Ochrona granicy (boundary defense)**  ***Wykrywanie/zapobieganie/poprawianie przepływu sieci przesyłających informacje o różnych poziomach zaufania z naciskiem na dane które mogą uszkodzić bezpieczeństwo.*** | |  | | |
|
| 12 | 12.1 | Sieć | Identyfikacja | Utrzymuj aktualny spis wszystkich granic sieci organizacji. | Utrzymuj aktualny spis wszystkich granic sieci organizacji. | X | X | X |
| 12 | 12.2 | Sieć | Wykrywanie | Skanuj w poszukiwaniu nieautoryzowanych połączeń przez granice zaufanej sieci | Wykonuj regularne skanowanie spoza każdej granicy sieci zaufanej, aby wykryć wszelkie nieautoryzowane połączenia, które są dostępne po drugiej stronie granicy. |  | X | X |
| 12 | 12.3 | Sieć | Ochrona | Odmów komunikacji ze znanymi złośliwymi adresami IP | Odmawiaj komunikacji ze znanymi złośliwymi lub nieużywanymi internetowymi adresami IP i ograniczaj dostęp tylko do zaufanych i niezbędnych zakresów adresów IP w każdej z granic sieci organizacji. |  | X | X |
| 12 | 12.4 | Sieć | Ochrona | Odmów komunikacji przez nieautoryzowane porty | Odmów komunikacji przez nieautoryzowane porty TCP lub UDP lub ruch aplikacji, aby zapewnić, że tylko autoryzowane protokoły mogą przekraczać granicę sieci do lub poza sieć w każdej z granic sieci organizacji. | X | X | X |
| 12 | 12.5 | Sieć | Wykrywanie | Skonfiguruj systemy monitorowania do nagrywania pakietów sieci | Skonfiguruj systemy monitorowania, aby rejestrować pakiety sieciowe przechodzące przez granicę w każdej z granic sieci organizacji. |  | X | X |
| 12 | 12.6 | Sieć | Wykrywanie | Konfiguruj systemy monitorowania do rejestrowanika pakietów sieciowych | Wdrażaj oparte na sieci czujniki wykrywania włamań (IDS) w celu wyszukania nietypowych mechanizmów ataku i wykrycia zagrożenia tych systemów w granicach sieci każdej organizacji. |  | X | X |
| 12 | 12.7 | Sieć | Ochrona | Wdrażaj sieciowe systemy zapobiegania włamaniom | Wdrażaj sieciowe systemy zapobiegania włamaniom (IPS), aby blokować złośliwy ruch sieciowy w każdej z granic sieci organizacji. |  |  | X |
| 12 | 12.8 | Sieć | Wykrywanie | Wdrażaj zbieranie NetFlow na urządzeniach sieciowych | Włącz gromadzenie danych NetFlow i rejestrowanie danych na wszystkich urządzeniach granicznych sieci. |  | X | X |
| 12 | 12.9 | Sieć | Wykrywanie | Używaj serwera proxy filtrującego warstwy aplikacji | Upewnij się, że cały ruch sieciowy do i z Internetu przechodzi przez uwierzytelnione proxy warstwy aplikacji, które jest skonfigurowane do filtrowania nieautoryzowanych połączeń. |  |  | X |
| 12 | 12.10 | Sieć | Wykrywanie | Odszyfruj ruch sieciowy w proxy | Odszyfruj cały zaszyfrowany ruch sieciowy na proxy granicznym przed analizą treści. Organizacja może używać białych list dozwolonych witryn, do których można uzyskać dostęp przez proxy bez odszyfrowywania ruchu. |  |  | X |
| 12 | 12.11 | Użytkownicy | Ochrona | Wymagaj by zdalne logowanie używało uwierzytelniania wieloczynnikowego | Wymagaj dostępu do zdalnego logowania do sieci organizacji w celu szyfrowania przesyłanych danych i korzystania z uwierzytelniania wieloczynnikowego. |  | X | X |
| 12 | 12.12 | Urządzenia | Ochrona | Zarządzaj wszystkimi urządzeniami zdalnie logującymi się w sieci wewnętrznej | Skanuj wszystkie urządzenia korporacyjne zdalnie logujące się do sieci organizacji przed uzyskaniem dostępu do sieci, aby upewnić się, że każda z zasad bezpieczeństwa organizacji została wymuszona w taki sam sposób, jak lokalne urządzenia sieciowe. |  |  | X |
| **13** | | | | **Ochrona danych**  ***Procesy i narzędzia wykorzystywane do zapobiegania eksfiltracji danych, łagodzą skutki eksfiltracji danych oraz zapewnieniają prywatność i integralność poufnych informacji.*** | |  | | |
|
| 13 | 13.1 | Dane | Identyfikacja | Prowadź spis poufnych informacji | Prowadź spis wszystkich poufnych informacji przechowywanych, przetwarzanych lub przesyłanych przez systemy technologiczne organizacji, w tym te znajdujące się on-site lub u zdalnego dostawcy usług. | X | X | X |
| 13 | 13.2 | Dane | Ochrona | Usuń dane poufne lub systemy, do których organizacja nie ma regularnego dostępu | Usuń poufne dane lub systemy, do których organizacja nie ma regularnego dostępu z sieci. Systemy te mogą być używane tylko jako samodzielne systemy (odłączone od sieci) przez jednostkę biznesową, która musi od czasu do czasu korzystać z systemu lub być całkowicie zwirtualizowana i wyłączona do czasu, aż będzie potrzebna. | X | X | X |
| 13 | 13.3 | Dane | Wykrywanie | Monitoruj i blokuj nieautoryzowany ruch sieciowy | Wdróż zautomatyzowane narzędzie na obwodach sieciowych, które monitoruje nieautoryzowany transfer poufnych informacji i blokuje takie transfery, jednocześnie ostrzegając specjalistów ds. bezpieczeństwa informacji. |  |  | X |
| 13 | 13.4 | Dane | Ochrona | Zezwalaj tylko na dostęp do autoryzowanych usług przechowywania w chmurze lub dostawców poczty e-mail. | Zezwalaj tylko na dostęp do autoryzowanych usług przechowywania w chmurze lub dostawców poczty e-mail. |  | X | X |
| 13 | 13.5 | Dane | Wykrywanie | Monitoruj i blokuj wszelkie nieautoryzowane użycie szyfrowania | Monitoruj cały ruch wychodzący z organizacji i wykrywaj nieautoryzowane użycie szyfrowania. |  |  | X |
| 13 | 13.6 | Dane | Ochrona | Szyfruj dane urządzenia mobilnego | Korzystaj z zatwierdzonych mechanizmów kryptograficznych w celu ochrony danych przedsiębiorstwa przechowywanych na wszystkich urządzeniach mobilnych. | X | X | X |
| 13 | 13.7 | Dane | Ochrona | Zarządzaj urządzeniami USB | Jeśli wymagane są urządzenia pamięci masowej USB, należy użyć oprogramowania korporacyjnego, które może skonfigurować systemy umożliwiające korzystanie z określonych urządzeń. Spis takich urządzeń powinien być stale prowadzony. |  | X | X |
| 13 | 13.8 | Dane | Ochrona | Zarządzaj konfiguracją zapisu/odczytu zewnętrznych nośników wymiennych | Skonfiguruj systemy, aby nie zapisywały danych na zewnętrznych nośnikach wymiennych, jeśli nie ma potrzeby biznesowej obsługi takich urządzeń. |  |  | X |
| 13 | 13.9 | Dane | Ochrona | Szyfruj dane na urządzeniach pamięci masowej USB | Jeśli wymagane są urządzenia pamięci masowej USB, wszystkie dane przechowywane na takich urządzeniach muszą być szyfrowane w spoczynku. |  |  | X |
| **14** | | | | **Kontrolowany dostęp na podstawie potrzebnych informacji**  ***Procesy i narzędzia wykorzystywane do śledzenia / kontroli / zapobiegania / poprawiania bezpiecznego dostępu do krytycznych zasobów (np. Informacji, zasobów, systemów) zgodnie z formalnym określeniem, które osoby, komputery i aplikacje mają potrzebę i prawo dostępu do tych krytycznych zasobów na podstawie zatwierdzonej klasyfikacji.*** | |  | | |
|
| 14 | 14.1 | Sieć | Ochrona | Segmentuj sieć na podstawie poufności | Segmentuj sieć na podstawie etykiety lub poziomu klasyfikacji informacji przechowywanych na serwerach, umieść wszystkie poufne informacje w oddzielnych wirtualnych sieciach lokalnych (VLAN). |  | X | X |
| 14 | 14.2 | Sieć | Ochrona | Włącz filtrowanie zapory między sieciami VLAN | Włącz filtrowanie zapory między sieciami VLAN, aby upewnić się, że tylko autoryzowane systemy będą w stanie komunikować się z innymi systemami niezbędnymi do wypełnienia określonych obowiązków. |  | X | X |
| 14 | 14.3 | Sieć | Ochrona | Wyłącz komunikację między stacjami roboczymi | Wyłącz komunikację między stacjami roboczymi, aby ograniczyć zdolność atakującego do przemieszczania się w bok i naruszania sąsiednich systemów za pomocą technologii takich jak prywatne sieci VLAN lub mikro segmentacja. |  | X | X |
| 14 | 14.4 | Dane | Ochrona | Szyfruj wszystkie poufne przesyłane informacje. | Szyfruj wszystkie poufne przesyłane informacje. |  | X | X |
| 14 | 14.5 | Dane | Wykrywanie | Wykorzystaj narzędzie Active Discovery do identyfikacji wrażliwych danych | Wykorzystaj aktywne narzędzie do wykrywania, aby zidentyfikować wszystkie poufne informacje przechowywane, przetwarzane lub przesyłane przez systemy technologiczne organizacji, w tym te znajdujące się “on-site” lub u dostawcy usług zdalnych, i aktualizuj poufne dane organizacji. |  |  | X |
| 14 | 14.6 | Dane | Ochrona | Chroń informacje poprzez listy kontroli dostępu | Chroń wszystkie informacje przechowywane w systemach z listami kontroli dostępu określonymi dla systemu plików, udziału sieciowego, roszczeń, aplikacji lub bazy danych. Kontrole te będą egzekwować zasadę, że tylko upoważnione osoby powinny mieć dostęp do informacji na podstawie ich potrzeby dostępu do informacji w ramach swoich obowiązków. | X | X | X |
| 14 | 14.7 | Dane | Ochrona | Wymuszaj kontrolę dostępu do danych przez zautomatyzowane narzędzia | Użyj zautomatyzowanego narzędzia, takiego jak Data Loss Prevention po stronie hosta, aby wymusić kontrolę dostępu do danych, nawet gdy dane są kopiowane z systemu. |  |  | X |
| 14 | 14.8 | Dane | Ochrona | Szyfruj poufne informacje w spoczynku | Szyfruj wszystkie poufne informacje w spoczynku za pomocą narzędzia, które wymaga dodatkowego mechanizmu uwierzytelniania, a który nie jest zintegrowany z systemem operacyjnym, w celu uzyskania dostępu do informacji. |  |  | X |
| 14 | 14.9 | Dane | Wykrywanie | Wymuszaj szczegółowe rejestrowanie w celu uzyskania dostępu lub zmiany poufnych danych | Wymuszaj szczegółowe rejestrowanie w celu uzyskania dostępu do poufnych danych lub zmian poufnych danych (przy użyciu narzędzi, takich jak monitorowanie integralności plików lub monitorowanie informacji o bezpieczeństwie i zdarzeniach). |  |  | X |
| **15** | | | | **Bezprzewodowa kontrola dostępu**  ***Procesy i narzędzia używane do śledzenia /kontroli /zapobiegania /poprawiania bezpieczeństwa korzystania z bezprzewodowych sieci lokalnych (WLAN), punktów dostępu i bezprzewodowych systemów klienta.*** | |  | | |
|
| 15 | 15.1 | Sieć | Identyfikacja | Prowadź spis autoryzowanych bezprzewodowych punktów dostępu | Zachowaj spis autoryzowanych bezprzewodowych punktów dostępu podłączonych do sieci przewodowej. |  | X | X |
| 15 | 15.2 | Sieć | Wykrywanie | Wykrywaj punkty dostępu bezprzewodowego podłączone do sieci przewodowej | Skonfiguruj narzędzia do skanowania luk w zabezpieczeniach sieci, aby wykrywać i ostrzegać o nieautoryzowanych punktach dostępu bezprzewodowego podłączonych do sieci przewodowej. |  | X | X |
| 15 | 15.3 | Sieć | Wykrywanie | Użyj systemu wykrywania włamań bezprzewodowych | Użyj bezprzewodowego systemu wykrywania włamań (WIDS), aby wykrywać i ostrzegać o nieautoryzowanych punktach dostępu bezprzewodowego podłączonych do sieci. |  | X | X |
| 15 | 15.4 | Urządzenia | Ochrona | Wyłącz dostęp bezprzewodowy na urządzeniach, jeśli nie jest wymagany | Wyłącz dostęp bezprzewodowy na urządzeniach, dla których dostęp bezprzewodowy nie ma celu biznesowego. |  |  | X |
| 15 | 15.5 | Urządzenia | Ochrona | Ogranicz dostęp bezprzewodowy do urządzeń klienckich | Skonfiguruj dostęp bezprzewodowy na komputerach klienckich, które mają zasadniczy cel, aby umożliwić dostęp tylko do autoryzowanych sieci bezprzewodowych i ograniczyć dostęp do innych sieci bezprzewodowych. |  |  | X |
| 15 | 15.6 | Urządzenia | Ochrona | Wyłącz możliwości sieci bezprzewodowej Peer-to-Peer na klientach bezprzewodowych | Wyłącz funkcje sieci bezprzewodowej peer-to-peer (ad hoc) na klientach bezprzewodowych. |  | X | X |
| 15 | 15.7 | Sieć | Ochrona | Wykorzystaj Advanced Encryption Standard (AES) do szyfrowania danych bezprzewodowych | Wykorzystaj Advanced Encryption Standard (AES) do szyfrowania przesyłanych danych bezprzewodowych. | X | X | X |
| 15 | 15.8 | Sieć | Ochrona | Użyj protokołów uwierzytelniania bezprzewodowego, które wymagają uwierzytelniania wieloczynnikowego | Upewnij się, że sieci bezprzewodowe używają protokołów uwierzytelniania, takich jak Extensible Authentication Protocol-Transport Layer Security (EAP / TLS), które wymagają wzajemnego uwierzytelniania wieloczynnikowego. |  |  | X |
| 15 | 15.9 | Urządzenia | Ochrona | Wyłącz bezprzewodowy dostęp peryferyjny urządzeń | Wyłącz bezprzewodowy dostęp peryferyjny urządzeń [takich jak Bluetooth i komunikacja bliskiego zasięgu (NFC)], chyba że taki dostęp jest wymagany do celów biznesowych. |  | X | X |
| 15 | 15.10 | Sieć | Ochrona | Utwórz oddzielną sieć bezprzewodową dla urządzeń osobistych i niezaufanych | Utwórz oddzielną sieć bezprzewodową dla urządzeń osobistych lub niezaufanych. Dostęp korporacyjny z tej sieci powinien być traktowany jako niezaufany i odpowiednio filtrowany i kontrolowany. | X | X | X |
| **16** | | | | **Monitorowanie i kontrola konta**  ***Aktywnie zarządzaj cyklem życia kont systemowych i aplikacyjnych - ich tworzeniem, używaniem, uśpieniem, usuwaniem - w celu zminimalizowania możliwości ich wykorzystania przez atakujących.*** | |  | | |
|
| 16 | 16.1 | Użytkownicy | Identyfikacja | Prowadź spis systemów uwierzytelniania | Prowadź spis każdego z systemów uwierzytelniania organizacji, w tym tych znajdujących się "on-site" lub u zdalnego dostawcy usług. |  | X | X |
| 16 | 16.2 | Użytkownicy | Ochrona | Skonfiguruj scentralizowany punkt uwierzytelniania | Skonfiguruj dostęp do wszystkich kont za pomocą kilku scentralizowanych punktów uwierzytelniania, w tym sieci, zabezpieczeń i systemów w chmurze. |  | X | X |
| 16 | 16.3 | Użytkownicy | Ochrona | Wymagaj uwierzytelniania wieloczynnikowego | Wymagaj uwierzytelniania wieloczynnikowego dla wszystkich kont użytkowników we wszystkich systemach, niezależnie od tego, czy jest zarządzany “on-site”, czy przez zewnętrznego dostawcę. |  | X | X |
| 16 | 16.4 | Użytkownicy | Ochrona | Szyfruj lub skracaj wszystkie dane uwierzytelniające | Zaszyfruj lub skracaj z saltem wszystkie dane uwierzytelniające podczas przechowywania. |  | X | X |
| 16 | 16.5 | Użytkownicy | Ochrona | Szyfruj przekazywanie nazwy użytkownika i danych uwierzytelniających | Upewnij się, że wszystkie nazwy użytkowników kont i dane uwierzytelniające są przesyłane przez sieci przy użyciu szyfrowanych kanałów. |  | X | X |
| 16 | 16.6 | Użytkownicy | Identyfikacja | Prowadź spis kont | Zachowaj spis wszystkich kont z systemu uwierzytelniania. |  | X | X |
| 16 | 16.7 | Użytkownicy | Ochrona | Stwórz proces unieważniania dostępu | Stwórz i przestrzegaj zautomatyzowanego procesu unieważniania dostępu do systemu poprzez wyłączenie kont natychmiast po zakończeniu lub zmianie obowiązków pracownika lub wykonawcy. Wyłączenie tych kont zamiast ich usuwania umożliwia zachowanie ścieżek audytu. |  | X | X |
| 16 | 16.8 | Użytkownicy | Odpowiedź | Wyłącz wszelkie niepowiązane konta | Wyłącz konto, które nie może być powiązane z procesem biznesowym lub właścicielem firmy. | X | X | X |
| 16 | 16.9 | Użytkownicy | Odpowiedź | Wyłącz konta nieaktywne | Automatycznie wyłączaj nieaktywne konta po określonym czasie bezczynności. | X | X | X |
| 16 | 16.10 | Użytkownicy | Ochrona | Upewnij się, że wszystkie konta mają datę wygaśnięcia | Upewnij się, że wszystkie konta mają datę wygaśnięcia, która jest monitorowana i egzekwowana. |  | X | X |
| 16 | 16.11 | Użytkownicy | Ochrona | Blokuj sesje stacji roboczej po bezczynności | Automatycznie blokuj sesje stacji roboczej po standardowym okresie bezczynności. | X | X | X |
| 16 | 16.12 | Użytkownicy | Wykrywanie | Monitoruj próby uzyskania dostępu do dezaktywowanych kont | Monitoruj próby uzyskania dostępu do nieaktywnych kont poprzez rejestrowanie audytowe. |  | X | X |
| 16 | 16.13 | Użytkownicy | Wykrywanie | Powiadamiaj o odchyleniach w zachowaniu użytkowników | Ostrzegaj, gdy zachowanie użytkowników podczas logowania odbiega od normalnego, takiego jak pora dnia, lokalizacja stacji roboczej i czas trwania. |  |  | X |
| **17** | | | | **Wdróż program podnoszenia świadomości i szkolenia w zakresie bezpieczeństwa**  ***Dla wszystkich ról funkcjonalnych w organizacji (ustalanie priorytetów dla tych, które mają kluczowe znaczenie dla biznesu i jego bezpieczeństwa), należy określić konkretną wiedzę, umiejętności i zdolności potrzebne do wspierania obrony przedsiębiorstwa; opracowywać i realizować zintegrowany plan oceny, identyfikacji luk i naprawiania poprzez politykę, planowanie, szkolenia i programy uświadamiające.*** | |  | | |
|
| 17 | 17.1 | N/A | N/A | Przeprowadź analizę luk umiejętności | Przeprowadź analizę luk w umiejętnościach, aby zrozumieć których umiejętności i zachowań członkowie personelu nie przestrzegają. Korzystając z tych informacji, stwórz podstawowy plan edukacji. |  | X | X |
| 17 | 17.2 | N/A | N/A | Zapewnij szkolenia | Zapewnij szkolenia w celu zidentyfikowania luki w umiejętnościach, aby pozytywnie wpłynąć na zachowania pracowników w zakresie bezpieczeństwa. |  | X | X |
| 17 | 17.3 | N/A | N/A | Stwórz program uświadamiający rolę bezpieczeństa | Stwórz program uświadamiający rolę bezpieczeństa dla wszystkich członków personelu, aby upewnić się, że rozumieją i wykazują niezbędne zachowania i umiejętności, aby zapewnić bezpieczeństwo organizacji. Program świadomości bezpieczeństwa organizacji powinien być przekazywany w sposób ciągły i angażujący pracowników. | X | X | X |
| 17 | 17.4 | N/A | N/A | Często aktualizuj program świadomości bezpieczeństwa | Upewnij się, że program świadomości bezpieczeństwa organizacji jest często aktualizowany (przynajmniej raz w roku) w celu uwzględnienia nowych technologii, zagrożeń, standardów i wymagań biznesowych. |  | X | X |
| 17 | 17.5 | N/A | N/A | Trenuj pracowników w zakresie bezpiecznego uwierzytelniania | Trenuj członków zespołu w zakresie znaczenia aktywowania i korzystania z bezpiecznego uwierzytelniania. | X | X | X |
| 17 | 17.6 | N/A | N/A | Szkolenie pracowników w zakresie ataków inżynierii społecznej | Wyszkol pracowników w zakresie identyfikacji różnych form ataków inżynierii społecznej, takich jak phishing, oszustwa telefoniczne i podszywanie się pod osoby. | X | X | X |
| 17 | 17.7 | N/A | N/A | Szkolenie pracowników o wrażliwej obsłudze danych | Trenuj członków personelu, jak identyfikować i właściwie przechowywać, przekazywać, archiwizować i niszczyć poufne informacje. | X | X | X |
| 17 | 17.8 | N/A | N/A | Trenuj pracowników o przyczynach niezamierzonego narażenia danych | Trenuj członków zespołu, aby byli świadomi przyczyn niezamierzonego narażenia danych, takich jak utrata urządzeń mobilnych lub wysłanie e-maila do niewłaściwej osoby z powodu autouzupełniania w wiadomości e-mail. | X | X | X |
| 17 | 17.9 | N/A | N/A | Trenuj członków personelu w zakresie identyfikacji i zgłaszania incydentów | Trenuj członków personelu, aby byli w stanie zidentyfikować najczęstsze wskaźniki incydentu i zgłosić taki incydent. | X | X | X |
| **18** | | | | **Bezpieczeństwo oprogramowania aplikacji**  ***Zarządzaj cyklem życia zabezpieczeń całego rozwijanego i zakupionego oprogramowania wewnętrznego, aby zapobiegać, wykrywać i korygować podatności w zabezpieczeniach.*** | |  | | |
|
| 18 | 18.1 | N/A | N/A | Ustal bezpieczne praktyki kodowania | Ustal bezpieczne praktyki kodowania odpowiednie dla używanego języka programowania i środowiska programistycznego. |  | X | X |
| 18 | 18.2 | N/A | N/A | Upewnij się, że przeprowadzane jest jawne sprawdzanie błędów dla całego oprogramowania rozwijanego przez firmę | W przypadku oprogramowania rozwijanego we własnym zakresie należy upewnić się, że przeprowadzane jest jawne sprawdzanie błędów i dokumentowane dla wszystkich danych wejściowych, w tym wielkość, typ danych i dopuszczalne zakresy lub formaty. |  | X | X |
| 18 | 18.3 | N/A | N/A | Sprawdź, czy zakupione oprogramowanie jest nadal obsługiwane | Sprawdź, czy wersja całego zakupionego oprogramowania jest obsługiwana przez programistę lub odpowiednio wzmocniona w oparciu o zalecenia dotyczące bezpieczeństwa. |  | X | X |
| 18 | 18.4 | N/A | N/A | Używaj tylko aktualnych i zaufanych komponentów firm trzecich | Do oprogramowania rozwijanego przez organizację używaj wyłącznie aktualnych i zaufanych komponentów firm trzecich. |  | X | X |
| 18 | 18.5 | N/A | N/A | Używaj tylko standaryzowanych i szeroko ocenianych algorytmów szyfrowania. | Używaj tylko standaryzowanych, obecnie akceptowanych i szeroko ocenianych algorytmów szyfrowania. |  | X | X |
| 18 | 18.6 | N/A | N/A | Upewnij się, że pracownicy z działu rozwoju oprogramowania są przeszkoleni w zakresie bezpiecznego kodowania | Upewnij się, że wszyscy pracownicy z działu rozwoju oprogramowania są przeszkoleni w pisaniu bezpiecznego kodu dla ich konkretnego środowiska programistycznego i obowiązków. |  | X | X |
| 18 | 18.7 | N/A | N/A | Zastosuj narzędzia statycznej i dynamicznej analizy kodu | Zastosuj narzędzia analizy statycznej i dynamicznej, aby sprawdzić, czy przestrzegane są bezpieczne praktyki kodowania dla oprogramowania rozwijanego wewnętrznie. |  | X | X |
| 18 | 18.8 | N/A | N/A | Stwórz proces akceptowania i zajmowania się raportami dotyczącymi luk w oprogramowaniu | Stwórz proces akceptowania i zajmowania się raportami dotyczącymi luk w oprogramowaniu, w tym umożliwienie zewnętrznym podmiotom skontaktowania się z grupą ds. bezpieczeństwa. |  | X | X |
| 18 | 18.9 | N/A | N/A | Oddziel systemy produkcyjne i nieprodukcyjne | Utrzymuj oddzielne środowiska dla systemów produkcyjnych i nieprodukcyjnych. Programiści nie powinni mieć niemonitorowanego dostępu do środowisk produkcyjnych. |  | X | X |
| 18 | 18.10 | N/A | N/A | Wdróż zapory sieciowe aplikacji | Chroń aplikacje internetowe, wdrażając firewalle aplikacji internetowych (WAF), które sprawdzają cały ruch przepływający do aplikacji w poszukiwaniu typowych ataków. W przypadku aplikacji, które nie są oparte na sieci Web, należy wdrożyć konkretne zapory sieciowe, jeśli takie narzędzia są dostępne dla danego typu aplikacji. Jeśli ruch jest szyfrowany, urządzenie powinno albo znajdować się za szyfrowaniem, albo być w stanie odszyfrować ruch przed analizą. Jeśli żadna z tych opcji nie jest odpowiednia, należy wdrożyć zaporę sieciową po stronie hosta. |  | X | X |
| 18 | 18.11 | N/A | N/A | Użyj standardowych szablonów konfiguracji hardowania dla baz danych | Dla aplikacji opartych na bazie danych użyj standardowych szablonów konfiguracji utwardzania (hardening). Wszystkie systemy będące częścią krytycznych procesów biznesowych również powinny zostać przetestowane. |  | X | X |
| **19** | | | | **Zarządzanie i reakcja na zdarzenia**  **C*hroń informacje organizacji, a także jej reputację, poprzez opracowanie i wdrożenie infrastruktury reagowania na incydenty (np. plany, zdefiniowane role, szkolenia, komunikacja, nadzór nad zarządzaniem) w celu szybkiego wykrywania ataku, a następnie skutecznego powstrzymania szkód i eliminacji atakującego oraz przywrócenia integralności sieci i systemów.*** | |  | | |
|
| 19 | 19.1 | N/A | N/A | Udokumentuj procedury reagowania na incydenty | Upewnij się, że zostały napisane plany reagowania na incydenty, które określają role personelu, jak również fazy obsługi/zarządzania incydentami. | X | X | X |
| 19 | 19.2 | N/A | N/A | Przypisz określone osoby do obsługi incydentów | Przypisz określone osoby do obsługi incydentów komputerowych i sieciowych oraz zapewnij śledzenie i dokumentację w trakcie incydentu. |  | X | X |
| 19 | 19.3 | N/A | N/A | Wyznacz personel zarządzający do obsługi obsługi incydentów | Wyznacz personel kierowniczy, a także personel dla kopii zapasowych, aby wspierać proces obsługi incydentów i pełnić kluczowe role decyzyjne. | X | X | X |
| 19 | 19.4 | N/A | N/A | Opracuj standardy dla zgłaszania incydentów obowiązujące w całej organizacji | Opracuj standardy obowiązujące w całej organizacji na czas potrzebny administratorom systemu i innym członkom personelu na zgłaszanie nieprawidłowych zdarzeń zespołowi zajmującemu się incydentami, a także opracuj mechanizmy takiego raportowania oraz rodzaje informacji, które powinny być zawarte w powiadomieniu o incydencie. |  | X | X |
| 19 | 19.5 | N/A | N/A | Gromadź informacje kontaktowe w celu zgłaszania incydentów związanych z bezpieczeństwem | Gromadź informacje na temat danych kontaktowych osób trzecich, które wykorzystasz do zgłaszania incydentów związanych z bezpieczeństwem, chodzi o dane do organó odpowiedzialnych za egzekwowanie prawa, odpowiednich departamentów rządowych, dostawców i partnerów Centrum Udostępniania Informacji i Analizy (ISAC). | X | X | X |
| 19 | 19.6 | N/A | N/A | Publikuj informacje dotyczące zgłaszania anomalii i incydentów | Publikuj informacje dla wszystkich członków personelu dotyczące zgłaszania anomalii i incydentów zespołowi, który tym się zajmuje. Takie informacje powinny być uwzględniane w rutynowych działaniach na rzecz świadomości pracowników. | X | X | X |
| 19 | 19.7 | N/A | N/A | Przeprowadzaj okresowe testowanie scenariuszy incydentów dla personelu | Planuj i przeprowadzaj rutynowe ćwiczenia incydentów, odpowiedzi i scenariuszy dla pracowników zaangażowanych w reakcję na incydent, aby utrzymać świadomość i gotowość reakcji na rzeczywiste zagrożenia. Ćwiczenia powinny testować kanały komunikacyjne, podejmowanie decyzji i reagowanie na incydenty techniczne za pomocą dostępnych narzędzi i danych. |  | X | X |
| 19 | 19.8 | N/A | N/A | Utwórz Schemat incydentów i ustalania priorytetów | Twórz schematy oceniania incydentów i ustalania priorytetów w oparciu o znany lub potencjalny wpływ na Twoją organizację. Wykorzystaj wynik do określenia częstotliwości aktualizacji statusu i procedur eskalacji. |  |  | X |
| **20** | | | | **Testy penetracyjne i ćwiczenia Red Team**  ***Sprawdź ogólną siłę obrony organizacji (technologia, procesy i ludzie), symulując cele i działania atakującego.*** | |  | | |
|
| 20 | 20.1 | N/A | N/A | Stwórz program testów penetracyjnych | Stwórz program do testów penetracyjnych, który obejmuje pełen zakres ataków mieszanych, takich jak ataki bezprzewodowe, oparte na kliencie i ataki aplikacji internetowych. |  | X | X |
| 20 | 20.2 | N/A | N/A | Przeprowadzaj regularne zewnętrzne i wewnętrzne testy penetracyjne | Przeprowadzaj regularne zewnętrzne i wewnętrzne testy penetracyjne w celu identyfikacji słabych punktów i wektorów ataku, które mogą zostać wykorzystane do skutecznego exploitu systemów korporacyjnych. |  | X | X |
| 20 | 20.3 | N/A | N/A | Wykonuj okresowe ćwiczenia Red Team | Wykonuj okresowe ćwiczenia Red Team, aby przetestować gotowość organizacyjną do identyfikowania i zatrzymywania ataków lub szybkiego i skutecznego reagowania. |  |  | X |
| 20 | 20.4 | N/A | N/A | Dołącz testy na obecność niezabezpieczonych informacji systemowych i artefaktów | Dołącz testy na obecność niezabezpieczonych informacji systemowych i artefaktów, które byłyby przydatne dla atakujących, w tym diagramy sieciowe, pliki konfiguracyjne, raporty ze starych testów penetracyjnych, wiadomości e-mail lub dokumenty zawierające hasła lub inne informacje krytyczne dla działania systemu. |  | X | X |
| 20 | 20.5 | N/A | N/A | Stwórz stanowisko testowe dla elementów które nie są zazwyczaj testowane w produkcji | Stwórz stanowisko testowe, które naśladuje środowisko produkcyjne dla konkretnych testów penetracyjnych i ataków Red Team na elementy, które zazwyczaj nie są testowane w produkcji, takie jak ataki na kontrolę nadzorczą i pozyskiwanie danych oraz inne systemy kontroli. |  | X | X |
| 20 | 20.6 | N/A | N/A | Korzystaj z narzędzi do skanowania podatności na atak i testów penetracyjnych. | Korzystaj z narzędzi do skanowania podatności na atak i testów penetracyjnych. Wyniki oceny skanowania narażenia na atak należy wykorzystać jako punkt wyjścia do ukierunkowania i skoncentrowania wysiłków testowania penetracji. |  | X | X |
| 20 | 20.7 | N/A | N/A | Upewnij się, że wyniki testu penetracyjnego są udokumentowane przy użyciu otwartych, odczytywalnych maszynowo standardów | Tam, gdzie to możliwe, upewnij się, że wyniki Red Team są dokumentowane przy użyciu otwartych, odczytywalnych maszynowo standardów (np. SCAP). Opracuj metodę punktacji do określania wyników ćwiczeń Red Team, aby wyniki można było porównywać w czasie. |  |  | X |
| 20 | 20.8 | N/A | N/A | Kontroluj i monitoruj konta powiązane z testami penetracyjnymi | Wszelkie konta użytkowników lub systemów używane do przeprowadzania testów penetracyjnych powinny być kontrolowane i monitorowane, aby upewnić się, że są one używane wyłącznie do legalnych celów i są usuwane lub przywracane do normalnego działania po zakończeniu testów. |  | X | X |