Co-funded by the Erasmus+ Programme of the European Union

Moduł szkoleniowy InCyT

Bezpieczeństwo informacji dla menedżerów Część 2, Tydzień 4 Moduł: Zarządzanie bezpieczeństwem informacji - 2	
Zajęcia edukacyjne	❑ **Webinar** ❑ **Ćwiczenia** ❑ **Warsztaty** ❑ **Prezentacje** ❑ **Inne**
Odpowiedzialni za zajęcia	• Fatma Gökdemir • Ali Gökdemir
Cele aktywności edukacyjnej	1. Ocena zagrożeń i podatności na zagrożenia 2. Zarządzanie zagrożeniami i lukami w zabezpieczeniach 3. Rodzaje oceny narażenia 4. Ciągłość operacji cybernetycznych 5. Zasoby cybernetyczne 6. Ocena skuteczności polityki bezpieczeństwa cybernetycznego
Umiejętności do zdobycia	• IS 1 • IS 3 • MS 5
Czas trwania okresu edukacyjnego	2 tygodnie
Wymagania wstępne	***Co jest potrzebne?***
	• Średniozaawansowane umiejętności obsługi komputera

Co-funded by the Erasmus+ Programme of the European Union

Krótka informacja o module

Opis
Zarządzanie zasobami zajmuje ważne miejsce w zakresie Systemu Zarządzania Bezpieczeństwem Informacji ISO 27001. W rzeczywistości identyfikacja i klasyfikacja zasobów informacyjnych jest jednym z pierwszych kroków konfiguracji bezpieczeństwa informacji. Identyfikacja i przypisanie wartości do zasobów w organizacji jest podstawowym krokiem w procesie analizy ryzyka. Spis zasobów jest przygotowywany w celu przypisania wartości do zasobów. Badanie rozpoznawcze obejmujące wszystkich pracowników powinno zostać przeprowadzone przed inwentaryzacją zasobów. Dzięki temu badaniu inwentaryzacja zasobów działu jest badana i wymieniana z możliwym ryzykiem i stopniem poufności. Inwentaryzacja zasobów powinna być przeprowadzana jeden po drugim na podstawie objętych nią procesów. Podczas przygotowywania inwentaryzacji zasobów; grupa zasobów, środowisko, w którym znajduje się określony składnik aktywów, kod klasyfikacji i obliczana jest wartość zasobów (poufność, integralność, dostępność). Zgodnie z wynikiem obliczeń określany jest status priorytetu i podejmowane są decyzje dotyczące działań. Po zakończeniu inwentaryzacji zasobów przygotowywana jest szczegółowa lista zapasów dla wykrytych zapasów oprogramowania i sprzętu. Warunki/kontrole dotyczące zarządzania zasobów w normie ISO27001 są zebrane w załączniku A.8. W tym module zbadamy warunki odpowiedzialności za aktywa zdefiniowane w A.8.1.

Treść materiału edukacyjnego

1. Ocena zarządzania bezpieczeństwem informacji

W pierwszym etapie zarządzania aktywami przydatne byłoby najpierw ujawnienie i wymienienie, jakie zasoby posiadamy. To, co instytucja ma lub czego nie ma, powinno być znane w pierwszej kolejności. Następnie należy zdefiniować ich własność. Żadna firma ani transakcja nie powinna pozostawać bez nadzoru. Następnie należy określić zasady korzystania z tych zasobów.

W celu uzyskania szczegółowych informacji na ten temat należy zbadać normę ISO27002. Oczekiwania dotyczące zarządzania zasobami w ISO27002 są zawarte w 8 artykule standardu:

Zarządzanie zasobami i odpowiedzialność za zasoby

Cel: Identyfikacja zasobów organizacji i zdefiniowanie odpowiednich obowiązków w zakresie ochrony.

1. Inwentaryzacja zasobów

Kontrola: Należy zidentyfikować zasoby związane z urządzeniami do przetwarzania informacji i informacji oraz sporządzić i prowadzić spis tych zasobów.

Przewodnik po aplikacjach: Organizacja powinna zidentyfikować odpowiednie zasoby w cyklu życia informacji i udokumentować ich znaczenie. Cykl życia informacji powinien obejmować tworzenie, przetwarzanie, przechowywanie, przesyłanie, usuwanie i niszczenie. Dokumentacja powinna być prowadzona zgodnie z istniejącymi zapasami lub konkretnie.

Inwentaryzacja zasobów; muszą być aktualne, spójne, dokładne i zgodne z innymi zapasami.

Własność zasobów powinna być przypisana do każdego zidentyfikowanego składnika zasobów (zob. art. 2) i należy określić jego klasę.

Inne informacje: Inwentaryzacja zasobów pomaga zapewnić skuteczną ochronę i może być również niezbędna do innych celów, takich jak zdrowie i bezpieczeństwo, ubezpieczenia lub finanse (zarządzanie zasobów).

Norma ISO/IEC 27005[11] zawiera przykłady zasobów, które mogą wymagać uwzględnienia przez organizację przy identyfikacji zasobów. Proces sporządzania spisu aktywów jest ważnym warunkiem wstępnym zarządzania ryzykiem (patrz ISO/IEC 27000 i ISO/IEC 27005).

2. Własność zasobów

Kontrola: Przypisanie właściciela musi być dokonane dla wszystkich zasobów przechowywanych w spisie.

Przewodnik po aplikacjach: Osoby fizyczne i inne podmioty z zatwierdzoną odpowiedzialnością kierownictwa za cykl życia zasobów kwalifikują się do wyznaczenia jako właściciele zasobów.

Proces jest często stosowany w celu zapewnienia, że własność zasobów jest określana w odpowiednim czasie. Własność musi zostać określona podczas tworzenia zasobów lub przenoszenia ich do organizacji. Właściciel składnika zasobów powinien być odpowiedzialny za właściwe zarządzanie zasobów przez cały cykl życia składnika zasobów.

Właściciel* zasobów*:

a) Zapewnić, że inwentaryzacja zasobów jest rejestrowana,

b) zapewnienia właściwej klasyfikacji i ochrony zasobów,

c) Definiowanie i okresowy przegląd ograniczeń dostępu do istotnych zasobów i ich klasyfikacji, z uwzględnieniem obowiązującej polityki kontroli dostępu,

d) Zapewnienie podjęcia odpowiednich działań w celu usunięcia lub zniszczenia zasobów.

Inne informacje: Może to być osoba fizyczna lub podmiot z zatwierdzeniem odpowiedzialności kierownictwa za kontrolowanie składnika zasobów przez cały jego cykl życia. Zidentyfikowany właściciel nie ma udziałów własnościowych w składniku zasobów.

Rutynowe zadania mogą być delegowane; (na przykład powiernik, który codziennie opiekuje się zasobem), ale odpowiedzialność spoczywa na właścicielu zasobów.

Identyfikacja grup zasobów w złożonych systemach informatycznych może być przydatna w zapewnianiu wspólnych funkcji. W takim przypadku ten właściciel usługi jest odpowiedzialny za świadczenie usługi, w tym za obsługę zasobów.

3. Dopuszczalne wykorzystanie zasobów

Kontrola: Zasady dotyczące dopuszczalnego wykorzystania informacji i zasobów związanych z informacjami i urządzeniami do przetwarzania informacji powinny zostać określone, udokumentowane i wdrożone.

Przewodnik po aplikacjach: Pracownicy i użytkownicy zewnętrzni, którzy korzystają z zasobów organizacji lub mają do nich dostęp, powinni być świadomi wymagań dotyczących bezpieczeństwa informacji dotyczących zasobów organizacji związanych z informacjami i urządzeniami do przetwarzania informacji oraz zasobami. Użytkownicy ci powinni być odpowiedzialni za korzystanie ze wszystkich zasobów przetwarzania informacji oraz za wszelkie wykorzystanie, które odbywa się na ich własną odpowiedzialność.

4. Zwrot zasobów

Kontrola: Wszyscy pracownicy i użytkownicy stron zewnętrznych muszą zwrócić wszystkie zasoby korporacyjne będące w ich posiadaniu po rozwiązaniu umowy o pracę, umowy lub porozumienia.

***Przewodnik po* aplikacji**: Proces wypowiedzenia powinien być sformułowany tak, aby obejmował zwrot własności wszystkich wcześniej przyznanych zasobów fizycznych i elektronicznych lub depozytów organizacji.

Gdy pracownik lub użytkownik zewnętrzny kupuje lub korzysta ze sprzętu organizacji, przestrzegane są procedury zapewniające, że wszystkie istotne informacje są przekazywane do organizacji i bezpiecznie usuwane ze sprzętu.

Jeśli pracownik lub użytkownik zewnętrzny ma informacje ważne dla bieżących operacji, informacje te muszą zostać udokumentowane i przekazane do organizacji.

W okresie wypowiedzenia organizacja; kontrolować nieautoryzowane kopiowanie powiązanych informacji, takich jak własność intelektualna, przez zwolnionych pracowników i kontrahentów.

2. Ocena zagrożeń i podatności na zagrożenia oraz zarządzanie nimi

Prawie każda organizacja ma wrażliwe i cenne zasoby, które należy chronić. Jednak nie każda organizacja ma kompleksową i w pełni przemyślaną strategię ochrony tych zasobów. W cyberbezpieczeństwie strategie zarządzania lukami w zabezpieczeniach są podstawą silnej obrony. Zazwyczaj strategie zarządzania lukami w zabezpieczeniach mają na celu pomoc systemom, sieciom, aplikacjom itp. Przyjmuje holistyczne i ciągłe podejście do zarządzania lukami w zabezpieczeniach Te luki są następnie identyfikowane, oceniane i naprawiane tak szybko, jak to możliwe.

Zagrożenia i trendy bezpieczeństwa stale ewoluują, co wymaga skutecznych, zapobiegawczych działań
w celu zarządzania zagrożeniami i lukami w zabezpieczeniach, które mogą zagrozić Twoim danym. Aby zidentyfikować wszystkie potencjalne cele naruszenia lub ataku, należy najpierw ograniczyć ryzyko poprzez przeprowadzenie inwentaryzacji aktywów. Cele muszą być następnie klasyfikowane i stale monitorowane pod kątem nowych potencjalnych luk w zabezpieczeniach. Model zagrożeń, który identyfikuje najcenniejsze zasoby organizacji o wysokim ryzyku, powinien zostać opracowany i przetestowany. Głównym celem procesu testowania zagrożeń i podatności (oceny) jest jak najlepsze zrozumienie krytyczności zasobów, luk w zabezpieczeniach tych zasobów oraz ograniczenie niezbędnych środków do skutecznej ochrony tych zasobów.

2.1. Co to jest ocena podatności?

Ocena luk w zabezpieczeniach to proces identyfikowania, identyfikowania, klasyfikowania i priorytetyzowania luk w zabezpieczeniach systemów komputerowych, aplikacji i infrastruktur sieciowych.

Oceny podatności zapewniają również organizacji wiedzę, świadomość i doświadczenie w zakresie ryzyka niezbędne do zrozumienia i reagowania na zagrożenia dla jej środowiska. Proces oceny podatności na zagrożenia ma na celu identyfikację zagrożeń i ryzyka, jakie stwarzają. Często wiążą się one z wykorzystaniem zautomatyzowanych narzędzi testowych, takich jak sieciowe skanery

bezpieczeństwa, których wyniki są wymienione w raporcie z oceny luk w zabezpieczeniach.

Organizacje dowolnej wielkości, nawet osoby o zwiększonym ryzyku cyberataków, mogą skorzystać z jakiejś formy oceny luk w zabezpieczeniach, ale duże organizacje i inne typy organizacji narażonych na ciągłe ataki skorzystają najbardziej na analizie luk w zabezpieczeniach.

Ponieważ luki w zabezpieczeniach mogą umożliwić hakerom uzyskanie dostępu do systemów i aplikacji informatycznych, niezwykle ważne jest, aby organizacje identyfikowały i naprawiały luki w zabezpieczeniach, zanim zostaną wykorzystane. Kompleksowa ocena luk w zabezpieczeniach w połączeniu z programem zarządzania może pomóc firmom poprawić bezpieczeństwo ich systemów.

2.2. Znaczenie ocen narażenia

Aby lepiej wyjaśnić znaczenie oceny podatności, rozważmy to oczami fizycznego właściciela nieruchomości. Jeśli jesteś właścicielem cennego budynku, prawdopodobnie podejmujesz szereg środków, aby go chronić: utrzymujesz go, ubezpieczasz i upewniasz się, że drzwi, okna są zamknięte, a alarmy są aktywowane. Wszystkie te kroki można określić jako zarządzanie ryzykiem dla nieruchomości i jej zawartości.

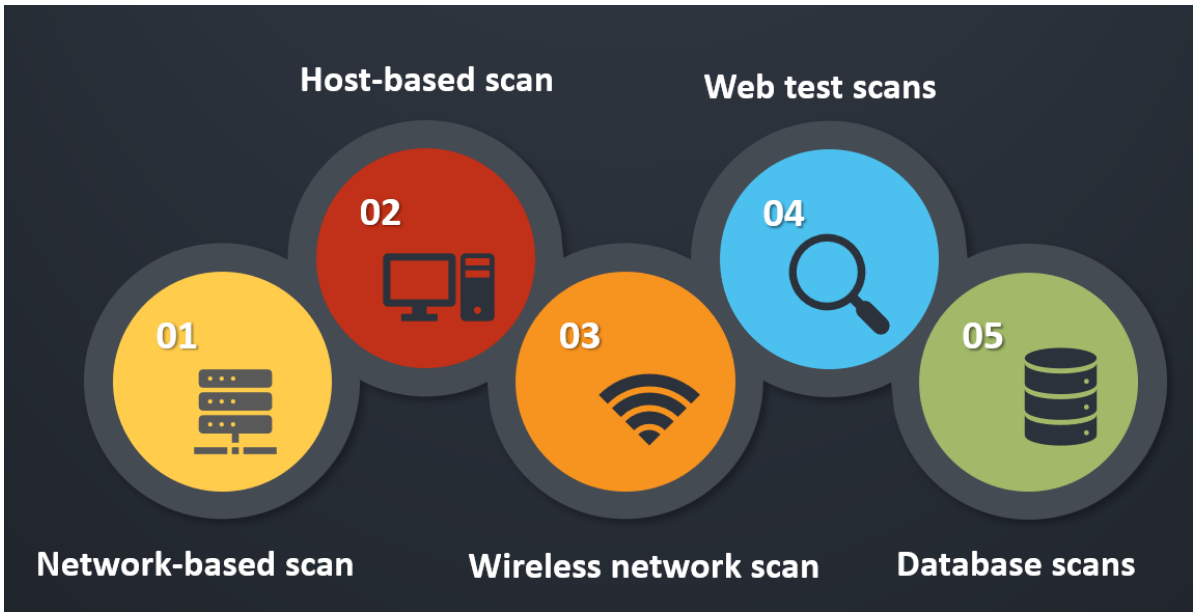
Co by było, gdybyś mógł zatrudnić kogoś do testowania i raportowania alarmów i zewnętrznych mechanizmów obronnych? Do luk w cyberbezpieczeństwie podchodzi się w podobny sposób. Zarządzanie lukami w zabezpieczeniach jest nadrzędną i ciągłą strategią, podczas gdy oceny podatności na zagrożenia są specyficznym narzędziem wykorzystywanym w tej szerszej strategii zarządzania.

Ocena luk w zabezpieczeniach zapewnia organizacji szczegółowe informacje na temat wszelkich słabych punktów zabezpieczeń w jej środowisku. Zawiera również wskazówki dotyczące sposobu oceny ryzyka związanego z tymi niedociągnięciami. Proces ten zapewnia organizacji lepsze zrozumienie jej zasobów, luk w zabezpieczeniach i ogólnego ryzyka, zmniejszając prawdopodobieństwo naruszenia przez cyberprzestępcę jej systemów i złapania firmy z zaskoczenia.

2.3. Rodzaje oceny narażenia

Oceny luk w zabezpieczeniach wykrywają różne luki w zabezpieczeniach systemu lub sieci. Oznacza to, że proces oceny obejmuje wykorzystanie różnych narzędzi, skanerów i metodologii do identyfikacji słabych punktów, zagrożeń i ryzyka.

Niektóre z różnych typów skanowania oceny luk obejmują (Rysunek 1):



Rys. 1. Rodzaje oceny narażenia

- **Skanowanie sieciowe** służy do identyfikowania potencjalnych ataków bezpieczeństwa sieci. Ten typ skanowania może również wykrywać zagrożone systemy w sieciach przewodowych lub bezprzewodowych.
- **Skanowanie oparte na hoście** służy do znajdowania i identyfikowania luk w zabezpieczeniach serwerów, stacji roboczych lub innych hostów sieciowych. Ten typ skanowania zwykle sprawdza porty i usługi, co można również zobaczyć w skanowaniu sieciowym. Zapewnia jednak lepszy wgląd w ustawienia konfiguracyjne i historię poprawek skanowanych systemów, w tym starszych systemów.
- **Skanowanie sieci** bezprzewodowych sieci Wi-Fi organizacji często koncentruje się na punktach ataku w infrastrukturze sieci bezprzewodowej. Oprócz identyfikowania nieuczciwych punktów dostępu, skanowanie sieci bezprzewodowej może również sprawdzić, czy sieć firmy jest bezpiecznie skonfigurowana.
- **Web skanuje** witryny testowe w celu wykrycia znanych luk w oprogramowaniu i błędnych konfiguracji w aplikacjach, sieci lub aplikacjach internetowych.
- **Skanowanie bazy danych** może identyfikować słabe punkty w bazie danych, aby zapobiec złośliwym atakom. Ataki polegające na wstrzykiwaniu kodu SQL.

2.4. Oceny podatności i testy penetracyjne

Ocena luk w zabezpieczeniach często obejmuje komponent testów penetracyjnych w celu zidentyfikowania luk w zabezpieczeniach personelu, procedur lub procesów organizacji. Oceny luk

w zabezpieczeniach mają wiele takich samych cech jak testy penetracyjne, ponieważ oba pozwalają organizacjom rygorystycznie badać swoje mechanizmy obronne. Luki te mogą zwykle nie zostać wykryte przez skanowanie sieci lub systemu. Proces ten jest czasami określany jako ocena podatności / testy penetracyjne lub **VAPT**.

Jednak testy penetracyjne nie są wystarczające jako pełna ocena podatności na zagrożenia i są w rzeczywistości oddzielnym procesem. Ocena podatności na zagrożenia ma na celu wykrycie luk w zabezpieczeniach w sieci i zaproponowanie odpowiedniego ograniczenia lub naprawy w celu ograniczenia lub wyeliminowania ryzyka.

Ocena luk w zabezpieczeniach wykorzystuje zautomatyzowane narzędzia do skanowania zabezpieczeń sieci. Wyniki są wymienione w raporcie z oceny luk w zabezpieczeniach, który koncentruje się na dostarczaniu organizacjom listy luk w zabezpieczeniach, które wymagają naprawy. Robi to jednak bez oceny konkretnych celów lub scenariuszy ataku.

Organizacje powinny regularnie przeprowadzać testy luk w zabezpieczeniach, aby zapewnić bezpieczeństwo swoich sieci, zwłaszcza w przypadku wprowadzania zmian. Na przykład testowanie powinno być wykonywane po dodaniu usług, zainstalowaniu nowego sprzętu lub otwarciu portów.

Natomiast testy penetracyjne polegają na identyfikowaniu luk w sieci i próbach wykorzystania ich do ataku na system. Chociaż czasami przeprowadza się je w połączeniu z ocenami podatności, głównym celem testów penetracyjnych jest sprawdzenie, czy luka rzeczywiście istnieje. Ponadto testy penetracyjne próbują udowodnić, że wykorzystanie luki w zabezpieczeniach może uszkodzić aplikację lub sieć.

Podczas gdy ocena luk w zabezpieczeniach jest zwykle zautomatyzowana w celu uwzględnienia szerokiej gamy niezałatanych luk w zabezpieczeniach, testy penetracyjne często łączą techniki automatyczne i ręczne, pomagając testerom w dalszym badaniu luk w zabezpieczeniach i wykorzystywaniu ich do uzyskania dostępu do sieci w kontrolowanym środowisku.

2.5. Zarządzanie lukami w zabezpieczeniach i zarządzanie ryzykiem

Podczas gdy zarządzanie lukami w zabezpieczeniach jest ciągłym procesem zarządzania lukami w zabezpieczeniach, zarządzanie ryzykiem ma szersze spojrzenie na wszystko, co może stanowić zagrożenie dla organizacji. Solidna strategia zarządzania ryzykiem pozwala na identyfikację, analizę i skuteczne ograniczanie ryzyka. Takie podejście pomaga organizacjom zrozumieć nie tylko istniejące luki w zabezpieczeniach, ale także skalę szkód, które mogą wystąpić w przypadku nadużycia. Ocena ryzyka i podatności na zagrożenia przeprowadzona pod parasolem zarządzania ryzykiem może zapewnić szczególnie szeroką perspektywę na siłę postawy bezpieczeństwa

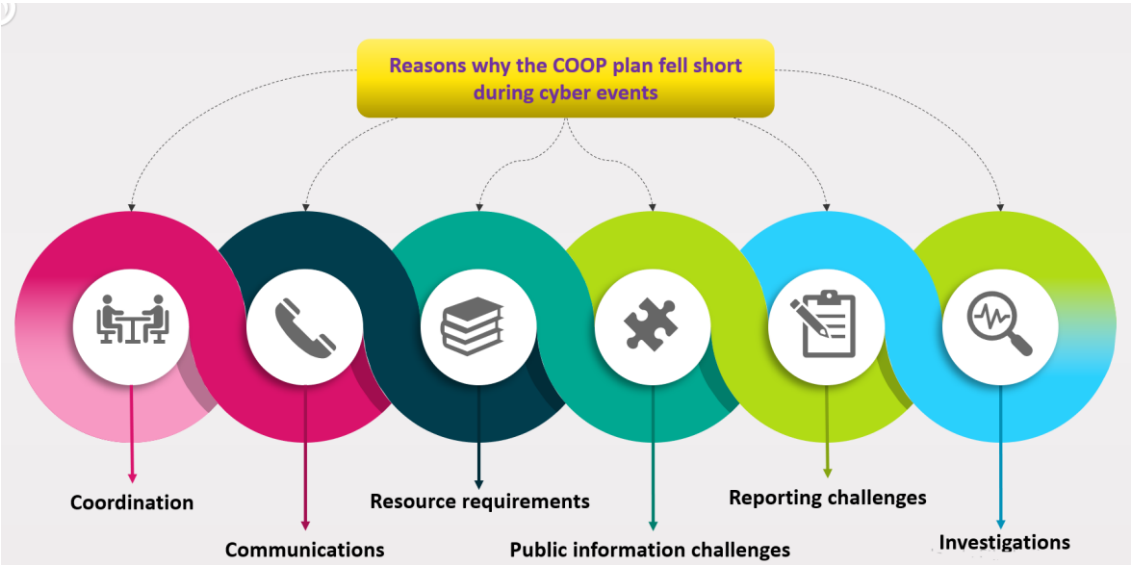
organizacji.

3. Ciągłość operacji cybernetycznych

Zwiększenie odporności na zagrożenia ze strony destrukcyjnego złośliwego oprogramowania wymaga wglądu w aktualny stan bezpieczeństwa, planowania i koordynowania kluczowych działań obronnych oraz prawidłowego dopasowywania kluczowych zasobów obronnych.

Incydenty cybernetyczne również zakwestionowały podstawowe wysiłki związane z planowaniem ciągłości. Podczas gdy wiele jurysdykcji posiada sprzęt i strategie identyfikacji, wykrywania i ochrony przed cyberatakami, znacznie mniej z nich przepracowało twarde realia ciągłości swoich operacji poprzez rzeczywisty atak. Kiedy cyberataki uderzają, wiele dotkniętych jurysdykcji stwierdza, że ich podstawowe plany COOP nie wytrzymują. Chociaż plany są wystarczające do przejścia do alternatywnego miejsca pracy, mają znacznie mniej do zaoferowania, jeśli chodzi o pracę bez dostępu do systemów i danych potrzebnych personelowi do wykonywania podstawowych funkcji zadań. W istniejących planach brakuje również specyfiki potrzebnej do ukierunkowania reakcji, a główne zainteresowane strony, takie jak członkowie personelu IT, często nie są zintegrowane ze strukturami reagowania. A plany nie są testowane pod kątem ćwiczeń lub incydentów w świecie rzeczywistym.

Tradycyjne plany COOP nie zapewniają ciągłości podczas incydentów cybernetycznych na kilka sposobów (rysunek 2):



Rys. 2. Powody, dla których plany COOP są niewystarczające dla ciągłości podczas zdarzeń cybernetycznych

Koordynacja: w tym kto jest zaangażowany w podejmowanie decyzji, jeśli chodzi o

oprogramowanie ransomware, decyzje o wyłączeniu systemów i decyzje o aktywacji jurysdykcyjnego Centrum Operacji Kryzysowych. Ponadto większość samorządów lokalnych nie ma wyraźnych poziomów eskalacji ataku ani powiązanych elementów akcji dla każdego poziomu. Przywództwo w reagowaniu i personel mogą być również niejasne; rodzaje wiedzy merytorycznej potrzebnej do przeprowadzenia społeczności przez incydent cybernetyczny różnią się od tych potrzebnych w przypadku ekstremalnych warunków pogodowych.

Komunikacja: w tym sposób, w jaki lokalni menedżerowie będą szybko dostarczać informacje pracownikom, gdy cyberatak poważnie zagrozi komunikacji. Obejmuje to zarówno natychmiastową komunikację wyjaśniającą, co zrobić, gdy rozpocznie się atak, jak i bieżącą komunikację, taką jak sposób wypłaty wynagrodzeń. Oba mają kluczowe znaczenie dla reakcji, a jednak oba mogą wymagać przekazania bez korzyści z typowych systemów łączności awaryjnej.

Wymagania dotyczące zasobów: które mogą się bardzo różnić od tych, które dotyczą bardziej tradycyjnej odpowiedzi. Na przykład personel może wymagać czystych komputerów, czystych serwerów, lokalnych drukarek, a nawet faksów i papieru. Co ważne, wymagania kadrowe mogą wzrosnąć jeszcze bardziej podczas odzyskiwania niż w odpowiedzi, ponieważ departamenty i agencje mają trudności z replikacją brakujących lub podejrzanych danych.

Wyzwania związane z informacją publiczną: Zgłoszenie urzędników ds. Informacji publicznej z niewielkim lub żadnym przeszkoleniem lub doświadczeniem w zakresie cyberbezpieczeństwa, brakiem wcześniej oskryptowanych komunikatów i brakiem zgody co do tego, kiedy informacje o ataku powinny zostać upublicznione. Dostarczanie informacji społeczeństwu ma kluczowe znaczenie, ponieważ obywatele martwią się o swoje dane i wiarygodność kluczowych systemów demokratycznych, takich jak głosowanie i wymiar sprawiedliwości.

Zgłaszanie wyzwań: To może opóźnić reakcję, ponieważ awarie nie są zgłaszane w spójny sposób, pozostawiając działy IT bez niezbędnego wspólnego obrazu operacyjnego, aby szybko zidentyfikować atak. Ponadto linie raportowania są często niejasne, a niewiele osób spoza IT rozumie, które systemy są połączone zarówno w obrębie jurysdykcji, jak i poza nią.

Dochodzenia: Dla wielu miejscowości jest to czarna skrzynka. Zaangażowanie jednej lub więcej organizacji federalnych oraz ograniczenia, jakie dochodzenia nakładają na działania naprawcze, nie są dobrze rozumiane ani planowane. To sprawia, że planowanie ciągłości jest niezwykle trudne, ponieważ istnieje niepewność co do tego, jak i kiedy naprawa może się w ogóle rozpocząć.

3.1. Priorytety natychmiastowego działania ze skoordynowaną obroną

• Opracuj cybernetyczną teczkę "weź i idź" z niezbędnymi procedurami i informacjami.

o Tworzenie mobilnych zestawów narzędzi bezpieczeństwa cybernetycznego, które obejmują procedury ustanawiania, wdrażania, utrzymywania i umożliwiania kontynuacji cyberodpornych TTP w ramach obiektu wyznaczonego przez COOP

• Opracowuj, testuj i weryfikuj podręczniki, role, obowiązki i narzędzia.

o Wyznacz konkretne role cybernetyczne, powiązane obowiązki i narzędzia cybernetyczne, które mogą zostać wdrożone w celu zapewnienia wdrożenia cyberCOOP.

o Zdefiniuj standardowe gry cyber COOP dla indywidualnej lub cybernetycznej realizacji zespołu za pomocą cybernetycznych narzędzi "Go Bag" i elastycznych TTP.

o Przeprowadzaj różne rodzaje ćwiczeń cybernetycznych (np. ćwiczenia typu mini-table top) za pomocą cybernetycznego "Go Bag" i podręcznika.

• Zdefiniuj procesy współpracy i zdobądź narzędzia dla cyberochronów i osób reagujących na incydenty.

o Zapewnienie, że zarówno mobilne, jak i stacjonarne procesy cyber-COOP obejmują komunikację i koordynację w celu promowania odpowiedniego zarządzania cyberobroną, synergii między wszystkimi działaniami reagowania oraz zmniejszenia luk w zakresie bezpieczeństwa podczas działań naprawczych.

Podczas gdy podstawowe plany COOP zwiększyły lokalną gotowość na wiele zagrożeń, z którymi borykają się jurysdykcje, są one niewystarczające w sytuacjach, które tworzą środowisko zupełnie inne niż norma. Ponieważ działy IT w całym kraju nadal dbają o to, aby systemy i dane były tak bezpieczne, jak to tylko możliwe, do menedżerów ds. sytuacji kryzysowych należy rozciągnięcie wyobraźni i zaplanowanie cyberataków, które poważnie wpływają na krytyczne systemy i dane.

3.2. Priorytety natychmiastowego działań w ramach reorganizacji

• Zidentyfikuj zależności zadań i funkcji biznesowych od zasobów cybernetycznych.

o Określ cele zadań zasobów, tak aby można było zidentyfikować i wyeliminować zastosowania zwiększające ryzyko bez żadnych odpowiednich korzyści z zadań.

✓ Zidentyfikuj i usuń lub zastąp strumieniowe źródła danych i połączenia, dla

których ryzyko przeważa nad korzyściami.

o Rozważ współzależności między funkcjami biznesowymi zadań i niezwiązanymi z zadaniem oraz organizacjami, które dzielą krytyczne role w dostarczaniu funkcji NEF.

- ✓ Realokacja zasobów lub ponowne przypisanie odpowiedzialności administracyjnej i zarządczej w oparciu o ryzyko do zadań i funkcji biznesowych.

• Zidentyfikuj zależności niezwiązane z zadaniem i funkcjami biznesowymi lub korzystające z zasobów cybernetycznych.

o Wykorzystaj analizę przepływu zadania, analizę zależności zadania i Red Teaming, aby odkryć nieudokumentowane zależności zadania.

o Przegląd i korelacja zadania i funkcji biznesowych z mapowaniem modeli zależności oraz działaniami i wynikami analizy wpływu.

o Identyfikacja systemów, aplikacji i procesów funkcji niekrytycznych oraz zasobów, które je obsługują.

- ✓ Oceń te funkcje pod kątem płynnej strategii wdrażania Cyber COOP, aby dostosować się do priorytetowych operacji i lepszego wykorzystania lub eliminacji zależności.

4. Zarządzanie zasobami cybernetycznymi, zmianami i konfiguracją

- ✓ **Zasób:** Zacznijmy od definicji zasobu. Słownikowa definicja zasobu jest użyteczną lub wartościową rzeczą lub osobą. Podobnie, zasobami dostawcy usług IT są jego narzędzia, aplikacje, elementy konfiguracji i wszelkie inne cenne elementy, które pomagają w dostarczaniu usług klientom lub firmom. Zasoby są częścią zarządzania zasobami usług i konfiguracją.
- ✓ **Element konfiguracji**: Element konfiguracji jest skracany jako CI, a element konfiguracji to dowolny składnik, którym należy zarządzać w celu dostarczenia usługi IT. Przykładami elementów konfiguracji są usługi IT, sprzęt, oprogramowanie, budynki, ludzie i dokumentacja formalna. Krótko mówiąc, każdy komponent lub element, który pomaga w dostarczeniu usługi IT klientowi, jest klasyfikowany jako element konfiguracji. Informacje o każdym elemencie konfiguracji są rejestrowane w rekordzie konfiguracji w systemie zarządzania konfiguracją, a informacje te są przechowywane przez cały cykl ich życia przez zarządzanie konfiguracją.
- ✓ **Baza danych zarządzania konfiguracją**: Baza danych zarządzania konfiguracją jest skracana jako CMDB. CMDB to baza danych służąca do przechowywania rekordów

konfiguracji przez cały ich cykl życia. CMDB przechowuje informacje o Twoich CI, z których każdy wyróżnia się unikalnym identyfikatorem, w tym informacje identyfikujące, takie jak numer seryjny, adres MAC lub adres IP; jego bieżąca wersja; jego lokalizacja; oraz informacje o dostawcy i dostawcy.

- ✓ **System zarządzania konfiguracją**: System zarządzania konfiguracją jest w skrócie CMS i jest zestawem narzędzi i baz danych, które są używane do zarządzania danymi konfiguracyjnymi dostawcy usług IT. Dane dotyczące elementów konfiguracji są przechowywane w rekordach konfiguracji, a rekordy konfiguracji są uwzględniane
  w bazach danych systemu zarządzania konfiguracją. CMDB dostawcy usług IT do zarządzania danymi konfiguracyjnymi są zawarte w procesie zarządzania zasobami usługi i konfiguracją. System zarządzania konfiguracją zawiera również informacje o incydentach, problemach, znanych błędach, zmianach i wydaniach, pracownikach, dostawcach, lokalizacjach, jednostkach biznesowych, klientach i użytkownikach. Podsumowując, wszystkie niezbędne informacje o elementach konfiguracji i zasobach IT są zawarte w Systemie Zarządzania Konfiguracją. W razie potrzeby informacje te są pozyskiwane z SYSTEMU CMS i odpowiednio wykorzystywane.

Zarządzanie konfiguracją, które jest zasadniczo definiowane jako proces identyfikacji, kontrolowania, monitorowania i audytu wprowadzonych zmian, jest krytyczną częścią silnego programu bezpieczeństwa. Zarządzanie zmianami i konfiguracją w organizacji ma silne powiązania z wymaganiami audytu w prawie wszystkich ramach i przepisach dotyczących zabezpieczeń.

Zarządzanie konfiguracją opiera się na kontroli i wydawaniu różnych wersji produktów. Domyślne konfiguracje systemów operacyjnych i aplikacji są zazwyczaj ukierunkowane na łatwość wdrażania i użytkowania, a nie na najlepsze praktyki w zakresie cyberbezpieczeństwa. Obecnie zarządzanie konfiguracją jest dyscypliną na żądanie o znaczących implikacjach dla cyberbezpieczeństwa, zwłaszcza że organizacje przechodzą od gotowych konfiguracji domyślnych do bezpieczniejszych konfiguracji aplikacji i sprzętu.

Dzisiaj zarządzanie konfiguracją oznacza różne rzeczy dla różnych osób. W niektórych implementacjach odnosi się do sposobu konfigurowania urządzeń sieciowych. W innych chodzi o wersję aplikacji, którą uruchamia zespół. Czasami ludzie w branży mylą zarządzanie zasobami IT z zarządzaniem zmianami i konfiguracją. Chociaż są podobne i równie ważne dla firmy, nie są takie same. Rozwiązania do zarządzania IT monitorują, optymalizują i zarządzają zasobami w całym stylu życia zasobów. Tymczasem CM zbiera, przechowuje, zarządza, aktualizuje i analizuje wszystkie elementy konfiguracji.

Podczas gdy wiele organizacji ma niedojrzałe programy CM, mają one kluczowe znaczenie dla

współczesnego krajobrazu cyberbezpieczeństwa i będą zyskiwać na znaczeniu wraz z ewolucją krajobrazu zagrożeń.

4.1. Zarządzanie konfiguracją i odzyskiwanie po awarii

Jeśli chodzi o nowoczesne odzyskiwanie po awarii, zarządzanie konfiguracją jest niezbędne. W przypadku katastrofy cyberbezpieczeństwa (w końcu 76% organizacji doświadczyło incydentu cyberbezpieczeństwa IoT) odzyskanie do najnowszej konfiguracji może być niemożliwe, jeśli nie ma dokumentacji tej konfiguracji.

To samo dotyczy cyberbezpieczeństwa: zespoły nie mogą wiedzieć, czy coś jest nie tak, jeśli nie ma ustandaryzowanego sposobu konfigurowania, zmieniania i dokumentowania środowiska cyfrowego.

4.2. Zarządzanie zmianami

Zarządzanie zmianami przebiega równolegle z zarządzaniem konfiguracją, chociaż te dwie **rzeczy *nie są*** takie same. Ludzie mylą je cały czas.
Podczas gdy zarządzanie konfiguracją to proces identyfikacji i dokumentowania komponentów sprzętowych i oprogramowania oraz powiązanych ustawień, zarządzanie zmianami jest podstawową funkcją większego procesu zarządzania konfiguracją. Zarządzanie zmianą odnosi się do powiązanych procesów i ma na celu stworzenie stabilności w systemie i zapobieganie niekontrolowanym lub przypadkowym zmianom lub dokumentowanie procesów zmian, gdy masz rotację w organizacji. Innymi słowy, pozwala firmom **planować zmiany**, a nie tylko na nie reagować.

4.2.1. Proces zarządzania zmianami

Dzisiaj dobrze zorganizowany proces zarządzania zmianą będzie obejmował:

- Przesyłanie żądań zmian
- Oceny ryzyka i skutków
- Zatwierdzanie/odrzucanie funkcji zmian
- Testowanie
- Funkcje planowania/powiadamiania użytkownika/szkolenia
- Implementacja
- Walidacja
- Dokumentacja

Jednym z miejsc, w których rozwija się zarządzanie zmianą, jest w przypadku decyzji awaryjnych, kiedy zmiany muszą zostać wprowadzone. Po wdrożeniu zmiany należy ją ponownie wprowadzić do procesu zarządzania zmianą, gdzie następnie skorzysta z już ustanowionych protokołów walidacji i dokumentacji.

4.3. Zarządzanie zasobami cyberbezpieczeństwa

Zarządzanie zasobami cyberbezpieczeństwa to proces gromadzenia danych o zasobach (urządzeniach, instancjach chmury i użytkownikach) w celu wzmocnienia podstawowych funkcji bezpieczeństwa, w tym:

- **Wykrywanie i reagowanie**: Zapewnienie możliwości wykrywania i reagowania zapewnia zasięg w całym przedsiębiorstwie
- **Zarządzanie lukami w zabezpieczeniach:** zrozumienie, które zasoby mogą być podatne na exploity, oraz upewnienie się, że wszystkie zasoby są oceniane pod kątem luk
  w zabezpieczeniach
- **Bezpieczeństwo w chmurze**: Zapewnienie, że instancje chmury są bezpieczne i skonfigurowane tak, aby zapobiegać nadmiernie dopuszczalnym prawom dostępu, nawet jeśli są one szybko uruchamiane i wycofywane z eksploatacji
- **Reagowanie na incydenty**: wykorzystanie wzbogaconych, skorelowanych danych o zasobach w celu przyspieszenia dochodzeń w sprawie reagowania na incydenty i działań naprawczych
- **Ciągłe monitorowanie kontroli:** Identyfikowanie, kiedy brakuje środków kontroli bezpieczeństwa i należy je zastosować

5. Ocena skuteczności polityki bezpieczeństwa cybernetycznego

Rozwój systemu informatycznego przebiega przez kilka odrębnych faz od analizy problemu aż po wdrożenie systemu. W trakcie tego procesu każdy krok jest dokumentowany za pomocą szeregu rezultatów, które obejmują studium wykonalności, a skończywszy na podręcznikach szkoleniowych i dokumentacji systemu. Przy opracowywaniu polityki bezpieczeństwa ten proces autodokumentacji na ogół nie występuje.

Wiele opracowanych obecnie polityk próbuje dopasować wszystko do polityki bezpieczeństwa: uzasadnienie ważności oraz szczegółowe instrukcje i opisy systemowe. Z pewnością sama polityka bezpieczeństwa jest już wystarczająco rozwlekła, bez szczegółów na temat tego, w jaki sposób dokument został stworzony, z kim konsultowano się przy jego tworzeniu lub w jaki sposób osiągnięto sformułowanie polityki. Nie będzie też żadnej dokumentacji problemów politycznych, które mogły wystąpić podczas wdrażania polityki, ani tego, jak szkolić ludzi w zakresie polityki. Jednak dzięki zastosowaniu technik dokumentacyjnych podczas opracowywania polityki polityka bezpieczeństwa może ponownie stać się dokumentem zasad. Inne kwestie niezwiązane z zasadami polityki bezpieczeństwa zostałyby udokumentowane gdzie indziej wraz z uzasadnieniem polityki.

Najważniejszą informacją, której często brakuje lub po prostu nieadekwatną, gdy próbujemy ocenić politykę bezpieczeństwa w organizacji, jest dokumentacja wymagań. Bez jasnego zrozumienia wymagań ocena jakości polityki bezpieczeństwa jest prawie niemożliwa. Analiza ryzyk/zagrożeń stojących przed organizacją to tylko część wymagań potrzebnych do opracowania polityki bezpieczeństwa. Równie ważne są cele organizacji i inne kwestie polityczne, które wpływają na rozwój, wdrażanie i akceptację polityki bezpieczeństwa. Dostępność obszernej dokumentacji, w tym wyników obszernej analizy wymagań, pozwoli na głębszą ocenę polityki bezpieczeństwa, a nie tylko powierzchowną ocenę produktu końcowego. Na przykład, zamiast koncentrować się tylko na tym, czy polityka została wdrożona w danym obszarze, ocena może teraz również uwzględniać, w jaki sposób obszar ten został opracowany w ramach polityki. Dokumentacja dowodowa może zostać oceniona w celu ustalenia, czy polityka odpowiednio obejmuje wszystkie kwestie zidentyfikowane w ramach rozwoju, nie osłabiając żadnego z nich. Jednak zasady bezpieczeństwa różnią się znacznie w zależności od kontekstu organizacji i można by oczekiwać, że ich rozwój również będzie się różnić. Istniałaby pewna wspólnota między politykami, nawet jeśli obszary docelowe uległyby dygresji. Jednak w przeciwieństwie do oceny produktu, wiele kryteriów w ocenie polityki bezpieczeństwa będzie miało charakter subiektywny. Wynika to z subiektywnego charakteru opracowywania polityki i środowiska, w którym polityka jest wdrażana.

5.1. Utrzymanie skuteczności polityk bezpieczeństwa IT

Technologia informacyjna lub IT jest prawdopodobnie technologią stulecia. To z pewnością zmieniło świat. Jednak przy wszystkich zaletach IT wiele zagrożeń bezpieczeństwa przeniknęło również do naszego życia. Organizacje muszą zaprojektować skuteczne zasady bezpieczeństwa informacji, aby zapewnić, że ich operacje biznesowe pozostaną bezpieczne przed złośliwymi intruzami i danymi do kradzieży. Jak na ironię, doskonałym sposobem na utrzymanie skuteczności polityk bezpieczeństwa wobec zmieniającego się krajobrazu ryzyka IT jest wykorzystanie większej ilości IT.

Oto niektóre ze sposobów, w jakie dział IT może utrzymać skuteczność zasad bezpieczeństwa:

- **Lepsza ocena ryzyka:** Ocena ryzyka bezpieczeństwa jest niezbędnym pierwszym krokiem w projektowaniu każdej polityki bezpieczeństwa informacji. Aby sprostać zagrożeniom wynikającym z szybko rozwijającego się sektora IT, IT jest jedynym antidotum. Ponieważ ryzyko stale się zmienia, IT jest koniecznością, aby utrzymać nowe zagrożenia w ryzach. Pozwala łatwo odkrywać nowe zagrożenia na podstawie poprzednich zapisów dotyczących zgodności, klasyfikować czynniki ryzyka oraz oceniać szkody, jakie może spowodować. Dlatego ważne jest, aby uczyć się na nowych osiągnięciach - dobrych lub złych - w IT.

Poprawi to ocenę ryzyka, a także gotowość na wypadek, gdyby zagrożenie było nieuchronne.

- **Lepsza zgodność**: dział IT pomaga monitorować, jak dobrze pracownicy i szefowie organizacji zachowują zgodność z organami regulacyjnymi, a także z zasadami bezpieczeństwa specyficznymi dla organizacji. Dzięki jednemu oprogramowaniu możesz mieć oko na autoryzacje dostępu, niezabezpieczone udostępnianie danych, niebezpieczne surfowanie po Internecie, niewystarczające szyfrowanie danych i niezliczone inne czynniki, które mogą poważnie wpłynąć na Twoje bezpieczeństwo.
- **Ciągła modernizacja jest koniecznością**: ponieważ świat IT zmienia się z każdym oddechem, musisz stale wypatrywać nowych zmian, które mogą złamać twój system. Monitoruj rozwój sytuacji w świecie cyberzagrożeń, cyberprzestępczości i bezpieczeństwa cybernetycznego. Często i regularnie uaktualniaj swoje zasady bezpieczeństwa informacji i oprogramowanie zabezpieczające, ponieważ mogą one bardzo szybko stać się nieaktualne. W ten sposób można zachować skuteczność zasad zabezpieczeń.
- **Szybkie łagodzenie**: Jeśli Twoja organizacja stoi w obliczu zbliżającego się zagrożenia bezpieczeństwa, które może prowadzić do potencjalnej utraty lub kradzieży danych, musisz mieć pod ręką plan łagodzenia skutków lub naprawy. Dział IT pomaga w planowaniu łagodzenia skutków w prosty i skuteczny sposób. Dzięki działowi IT można przypisywać i łączyć kroki ograniczania ryzyka z różnymi potencjalnymi zagrożeniami podczas projektowania zasad zabezpieczeń. Dzięki temu łagodzenie będzie terminowe i skuteczniejsze, a tym samym utrzyma skuteczność zasad bezpieczeństwa.
- **Zwiększona odpowiedzialność**: Żadna polityka informacyjna nie może pozostać skuteczna, jeśli ludzie nie są odpowiedzialni za ryzyko, zgodność i łagodzenie. IT ułatwia zapewnienie rozliczalności działań naprawczych. Może znacznie poprawić widoczność ryzyka i ocenę dojrzałości, zgodność i środki zaradcze podejmowane przez organizację. Oznacza to, że Twoi pracownicy będą bardziej szybcy i bardziej odpowiedzialni za kroki wymienione w polityce bezpieczeństwa informacji.

5.2. Ocena zagrożeń bezpieczeństwa

Ocena ryzyka, po ustaleniu, które aktywa informacyjne będą chronione, wybierana jest metoda oceny ryzyka i definiowane są ryzyka. Zgodnie z wybraną metodą oceny ryzyka aktywa informacyjne są pozycjonowane na mapie ryzyka pokazanej na rysunku. Po dokonaniu oceny mapa oceny ryzyka obejmuje procesy poprawy i kontroli ryzyka dla zagrożeń o dużym wpływie i prawdopodobieństwie. Ponieważ lokalizacja aktywów informacyjnych na mapie ryzyka może ulec zmianie, mapa oceny ryzyka powinna być regularnie aktualizowana i należy podjąć niezbędne środki ostrożności.

Ryzyko definiuje się jako kombinację prawdopodobieństwa zdarzenia i jego wyniku. Ocena ryzyka,

która jest etapem zarządzania ryzykiem, jest procesem, w którym definiowane są ryzyka oraz określane są skutki i priorytety zidentyfikowanego ryzyka. Zarządzanie ryzykiem polega na określeniu akceptowalnego poziomu ryzyka, ocenie bieżącego ryzyka, podjęciu niezbędnych kroków w celu zmniejszenia tego ryzyka do akceptowalnego poziomu i utrzymaniu tego poziomu ryzyka. Informacje i inne zasoby, zagrożenia dla tych zasobów, luki w istniejącym systemie i kontrole systemu bezpieczeństwa to składniki, które określają bieżące ryzyko. Identyfikacja informacji lub aktywów, które wymagają ochrony; określenie, jak cenne są te aktywa dla zakładów; ujawnienie, które ze znanych i możliwych zagrożeń dla tych aktywów będą próbowane w celu zapobieżenia; badanie, w jaki sposób mogą wystąpić ewentualne straty; określenie zakresu możliwych zagrożeń dla każdego składnika aktywów; Badanie tego, co można zrobić w pierwszej kolejności, aby zmniejszyć zakres i prawdopodobieństwo strat, które mogą wystąpić w tych aktywach, oraz planowanie kroków, które należy podjąć, aby utrzymać zagrożenia wybiegające w przyszłość na minimalnym poziomie, to pewne fazy oceny ryzyka. Koszt systemu bezpieczeństwa, który ma zostać ustanowiony i wdrożony w wyniku zarządzania ryzykiem, jest kolejną ważną kwestią, którą należy wziąć pod uwagę. Koszt systemu bezpieczeństwa powinien być ograniczony wartością chronionych informacji oraz ryzykiem określonym poprzez badanie możliwych zagrożeń. Wraz z zasadą, że nie będzie 100% bezpieczeństwa, idealna konfiguracja bezpieczeństwa informacji jest realizowana poprzez trzy procesy. Procesy te to zapobieganie, wykrywanie i reagowanie (reakcja).

Zapobieganie; Jest to proces, na którym systemy bezpieczeństwa koncentrują się i działają najbardziej. Opracowywane są różne środki mające na celu izolację systemu przed zagrożeniami i atakami na systemy komputerowe, takie jak środki bezpieczeństwa stosowane w życiu codziennym, takie jak ogrodzenie ogrodu domowego i użycie stalowych drzwi. Jeśli chodzi o bezpieczeństwo komputera osobistego, zainstalowanie programów do skanowania antywirusowego, wykonywanie tych programów i dodatków Service Pack dla systemu operacyjnego oraz korekcję błędów i aktualizacje w regularnych odstępach czasu, korzystanie z chronionego hasłem wygaszacza ekranu na komputerze, blokowanie systemu po długim przebywaniu z dala od komputera, oszacowanie używanych haseł jest trudne, ustalanie, utrzymywanie tych haseł w tajemnicy i zmienianie ich w regularnych odstępach czasu, uważanie na udostępnianie dysków, zwracanie uwagi na pliki pobierane z Internetu lub wysyłane pocztą elektroniczną, zabezpieczanie ważnych dokumentów hasłem lub utrzymywanie ich w postaci zaszyfrowanej, poufne wiadomości e-mail lub ważne informacje, witryny bez certyfikatów bezpieczeństwa. Niektóre środki, które mogą wydawać się proste, ale ratują życie, takie jak nie wysyłanie za pomocą niebezpiecznych środków, wyłączanie dostępu do Internetu, gdy nie jest używany, regularne tworzenie kopii zapasowych ważnych informacji i dokumentów. Kroki zapobiegawcze, które należy wdrożyć w zakresie bezpieczeństwa komputerowego w środowiskach korporacyjnych, są szersze i bardziej złożone. Niektóre z rzeczy, które są wykonywane w celu zapobiegania w takich systemach, w których pracują eksperci ds.

Bezpieczeństwa:

- Okresowe przeglądy dodatków Service Pack oraz aktualizacji systemu operacyjnego i oprogramowania,
- Ograniczenie praw użytkownika do minimum, nie uruchamianie nieużywanych protokołów, usług, komponentów i procesów,
- Techniki szyfrowania w transmisji danych, skanery podatności,
- Korzystanie z wirtualnej sieci prywatnej,
- Wykorzystanie infrastruktury klucza publicznego i podpisu elektronicznego można wymienić jako wykorzystanie systemów biometrycznych.

W rzeczywistości, jeśli postęp określony w procesie zapobiegania mógłby być doskonały, dalsze procesy nie byłyby w ogóle potrzebne. W najgorszym wypadku wszystkim atakom można by zapobiec. Ale żaden produkt zabezpieczający nie jest doskonały ani kompletny. Ponadto prawie codziennie wykrywane są różne luki w systemach transmisji, usługach internetowych, technologiach internetowych i aplikacjach bezpieczeństwa. Z tego punktu widzenia wzrasta wykorzystanie procesów wykrywania i dopasowywania.

Oznaczanie; Bezpieczeństwo to nie tylko kwestia zapobiegania. Na przykład fakt, że muzeum jest dobrze chronione, że muzeum jest otoczone płotami, że drzwi są zamknięte i zamknięte, nie wymaga używania strażników w nocy w tym muzeum. W ten sam sposób zwiększa się również wykorzystanie metod wykrywania prób ataku na systemy komputerowe. Zapobieganie to budowanie bariery, która albo wzmacnia ataki (ale nie uniemożliwia), albo zniechęca (ale nie niszczy) napastników. Zapobieganie bez wykrycia i reakcji może przynieść jedynie ograniczone korzyści. Gdyby tylko zapobieganie było wystarczające, większość ataków nie byłaby nawet znana. Dzięki wykryciu można zgłaszać wcześniej znane lub nowo pojawiające się ataki i udzielać im odpowiednich odpowiedzi. Pierwszym i najbardziej podstawowym krokiem w wykrywaniu jest monitorowanie całego stanu i ruchu systemu oraz prowadzenie zapisów tych informacji. W ten sposób zbierane są również dane i dowody do analizy po ataku. Zapory ogniowe, systemy wykrywania włamań, monitory ruchu sieciowego, skanery portów, użycie honeypot, narzędzia antywirusowe i szpiegujące w czasie rzeczywistym, programy kontroli sum kontrolnych plików i sieciowe czujniki Sniffera to jedne z najczęstszych metod stosowanych w procesie wykrywania.

AnswerBack; Tak jak miejsce wyposażone w strażników, psy, kamery bezpieczeństwa, czujniki może przyciągnąć uwagę złodziei, tak systemy komputerowe z systemami wykrywania w czasie rzeczywistym są również atrakcyjne dla hakerów i napastników. Szybka reakcja jawi się jako niezbędny element, który uzupełnia system bezpieczeństwa w celu odparcia tych ataków. Odpowiedź można zdefiniować jako wykonanie działań, które zareagują natychmiast lub tak szybko, jak to możliwe, na próby ataku, które nie mogą być rozwiązane przez proces zapobiegania i określone przez procesy wykrywania. Systemy wykrywania włamań mogą mieć sens, jeśli istnieje

ktoś lub system, który reaguje na to wykrycie. W przeciwnym razie sytuacja ta nie wykracza poza korzyść alarmu samochodowego, którego nikt nie słyszy i nie dba o to. Pod tym względem wzajemność jest ważnym ogniwem, które uzupełnia proces bezpieczeństwa. Nawet jeśli atakowi nie można całkowicie zapobiec; Pozwala systemowi powrócić do normalnego stanu, zidentyfikować przyczyny ataku, złapać atakującego w razie potrzeby, zidentyfikować luki w systemie bezpieczeństwa oraz zreorganizować procesy zapobiegania, wykrywania i reagowania. Zaplanowanie działań, które należy podjąć po wykryciu ataku, z wyprzedzeniem zapewni, że proces ten będzie działał skutecznie i nie będzie marnował czasu i pieniędzy. Odzyskiwanie po awarii znajduje się w czołówce głównych planów najgorszych przypadków podjętych na tym etapie.

Pytania:

1. Który z poniższych nie jest jednym z etapów zarządzania aktywami.

A) Sporządzenie spisu zasobów

B) Ustalenie własności zasobów

C) Określenie rachunku kosztów

D) Określenie zasad użytkowania zasobów

2. Jaki jest główny cel procesu testowania zagrożeń i luk w zabezpieczeniach?

A) Aby jak najlepiej zrozumieć luki w zabezpieczeniach zasobów i podjąć niezbędne środki w celu skutecznej ochrony tych aktywów.

B) Zarządzanie lukami w zabezpieczeniach

C) Uzyskanie wstępnej informacji o inwentaryzacji aktywów

D) Zamykanie luk w zabezpieczeniach

3. Która z poniższych sytuacji nie jest rodzajem oceny narażenia?

A) Skanowanie sieciowe

B) Skanowanie oparte na hoście

C) Skanowanie bazy danych

D) Skanowanie oparte na serwerze

4. Który z poniższych elementów nie jest jednym z poniższych procesów zarządzania zasobami cyberbezpieczeństwa?

A) Zarządzanie lukami w zabezpieczeniach

B) Zarządzanie kosztami

C) Ciągłe monitorowanie kontroli

D) Wykrywanie i interwencja

5. Które z poniższych rozwiązań nie jest sposobem na utrzymanie przez dział IT skuteczności jego polityki bezpieczeństwa?

A) Ocena ryzyka

B) Ciągła modernizacja

C) Szybkie łagodzenie

D) Polityka bezpieczeństwa

6. Który z poniższych procesów nie jest jednym z trzech procesów, które stanowią idealną konfigurację bezpieczeństwa informacji?

A) Przygotowanie

B) Zapobieganie

C) Określenie

D) Odpowiedź zwrotna

Pytania samooceny. Po udzieleniu odpowiedzi uczeń może zobaczyć wyniki i porównać je z tymi zapisanymi na platformie

- Czym jest podatność systemów informatycznych
- Wyjaśnij i podaj przykład zarządzania lukami w zabezpieczeniach i zarządzania ryzykiem

Załączniki (prezentacja PowerPoint, materiały informacyjne, wydruki, linki, wideo...):

Zobacz załączniki

Referencje:

1. Evaluating IS Security Policy Development S.B. Maynard1 & A.B. Ruighaver2 Department of Information Systems University of Melbourne Australia
2. https://www.bizzsecure.com/how-it-can-maintain-the-effectiveness-of-security-policies/
3. https://blog.masterofproject.com/service-asset-and-configuration-management/
4. https://www.apptega.com/blog/change-configuration-management-cybersecurity
5. https://cam.scmagazine.com/it-service-management-vs-cybersecurity-asset-management/
6. http://www2.mitre.org/public/industry-perspective/documents/06-ar-cyber-coop-planning.pdf
7. https://icma.org/articles/pm-magazine/cyber-continuity-planning-go-big-or-go-home
8. https://www.kroll.com/en/services/security-risk-management/security-consulting/threat-vulnerability-assessments
9. https://www.xmcyber.com/blog/what-is-the-difference-between-vulnerability-assessment-and-vulnerability-management/
10. https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis