Szkolenie: Compendium CE

KSC/NIS2: Cyberhigiena - zasady bezpiecznej pracy na co dzień - szkolenie dla wszystkich pracowników

Cel szkolenia:

Szkolenie rozwija praktyczne nawyki cyberhigieny potrzebne do bezpiecznej pracy na co dzień. Uczestnicy poznają znaczenie poufności, integralności i dostępności informacji w realiach procesów biznesowych, najczęstsze scenariusze ataków (w tym socjotechnikę, phishing/BEC, malware i wycieki danych) oraz zasady bezpiecznej obsługi poczty, haseł i dostępu. Omawiane są także standardy pracy zdalnej i mobilnej, ścieżki zgłaszania incydentów (w tym presja czasowa 24h/72h) oraz konsekwencje organizacyjne i odpowiedzialność pracownika.

Cele szkolenia:

- Identyfikacja współczesnych cyberzagrożeń: Rozpoznawanie mechanizmów phishingu, ataków typu Business Email Compromise (BEC), metod socjotechnicznych (np. „oszustwo na prezesa”) oraz zagrożeń płynących ze strony złośliwego oprogramowania (ransomware).
- Praktyczna implementacja zasad cyberhigieny: Skuteczne zarządzanie tożsamością (silne uwierzytelnianie, MFA), zasady bezpiecznej komunikacji i pracy w sieci, ochrona nośników danych oraz dbałość o aktualność systemów.
- Procedury reagowania na incydenty: Znajomość ścieżek raportowania podejrzenia naruszeń, zabezpieczanie dowodów cyfrowych oraz podejmowanie działań ograniczających eskalację szkód.
- Budowanie kultury bezpieczeństwa: Zrozumienie biznesowych, prawnych i organizacyjnych konsekwencji incydentów oraz roli pracownika jako kluczowego ogniwa w systemie ochrony informacji.

Grupa docelowa:

Wszyscy pracownicy oraz współpracownicy (B2B, stażyści) wykorzystujący w codziennej pracy zasoby IT, pocztę elektroniczną oraz systemy informatyczne organizacji.

Plan szkolenia:

- Wprowadzenie: Znaczenie cyberhigieny w organizacji
  - Praktyczna implementacja triady bezpieczeństwa: Operacyjne ujęcie poufności, integralności i dostępności informacji w codziennych procesach biznesowych.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Analiza wektorów socjotechnicznych: Sposoby wykorzystywania przez napastników pośpiechu oraz rutyny pracowników w celu przełamania barier bezpieczeństwa.

- Przegląd współczesnych cyberzagrożeń i scenariuszy ataków
  - Socjotechnika i kompromitacja tożsamości: Mechanizmy phishingu i smishingu, wykorzystanie fałszywych paneli logowania oraz ataki typu Business Email Compromise (BEC) i Deepfake.
  - Złośliwe oprogramowanie (Malware): Analiza wektorów infekcji oraz procesów szyfrowania danych dla celów wymuszeń.
  - Naruszenia poufności i wycieki informacji: Incydenty wynikające z błędów ludzkich (błędny adresat), nieautoryzowanego udostępniania zasobów oraz błędów konfiguracyjnych w środowiskach chmurowych.
- Praktyki cyberhigieny w codziennych procesach operacyjnych
  - Zarządzanie tożsamością i dostępem: Wykorzystanie korporacyjnych menedżerów haseł, obligatoryjne stosowanie uwierzytelniania wieloskładnikowego (MFA) oraz fizyczne zabezpieczanie stanowisk pracy.
  - Bezpieczna obsługa korespondencji i zasobów cyfrowych: Weryfikacja integralności załączników (makra, dokumenty PDF) oraz analiza odnośników w celu eliminacji ryzyk socjotechnicznych.
  - Utrzymanie standardów bezpieczeństwa urządzeń: Systematyczne wdrażanie aktualizacji systemowych oraz zachowanie ścisłej separacji pomiędzy zasobami służbowymi a prywatnymi.
  - Kontrola uprawnień: Implementacja zasady minimalnych przywilejów (Least Privilege) oraz ograniczanie dostępu do informacji zgodnie z regułą „need-to-know”.
- Standardy bezpieczeństwa pracy zdalnej i mobilnej
  - Ochrona kanałów komunikacji i otoczenia: Bezpieczne korzystanie z sieci bezprzewodowych (Wi-Fi, hotspoty), obligatoryjne stosowanie tuneli VPN oraz zachowanie poufności rozmów i ochrony wizualnej ekranu w przestrzeni publicznej.
  - Zarządzanie fizycznymi nośnikami i dokumentacją: Ścisłe procedury ochrony wydruków i wymiennych nośników danych oraz zapobieganie nieautoryzowanemu utrwalaniu informacji (np. poprzez zdjęcia ekranów).
  - Procedury incydentowe: Ścieżka natychmiastowego raportowania kradzieży lub utraty sprzętu służbowego w celu zdalnej blokady zasobów i mitygacji skutków naruszenia.
- Procedury reagowania na incydenty (wytyczne dla personelu)
  - Identyfikacja i klasyfikacja zdarzeń: Umiejętność rozpoznawania sytuacji stanowiących incydenty bezpieczeństwa w obszarach fizycznych, logicznych i administracyjnych.
  - Protokół zgłoszeniowy i ograniczenie eskalacji: Wytyczne dotyczące niezwłocznego raportowania zdarzeń wyznaczonymi kanałami pod krytyczną presją czasu wynikającą z terminów ustawowych (24h/72h).
  - Zabezpieczenie materiału dowodowego: Praktyczne metody dokumentowania incydentów bezpieczeństwa na potrzeby analizy po włamaniowej oraz działań śledczych.
- Analiza skutków naruszeń i ramy odpowiedzialności
  - Wielowymiarowy wpływ incydentów na organizację i personel: Identyfikacja konsekwencji

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

operacyjnych (przestoje procesów), finansowych (koszty mitygacji) oraz wizerunkowych, przy jednoczesnym zrozumieniu zakresu odpowiedzialności indywidualnej pracownika.
    - Uzasadnienie stosowania wewnętrznych mechanizmów kontrolnych: Rola polityk bezpieczeństwa oraz procesów klasyfikacji informacji jako narzędzi zapewniających zgodność z wymogami prawnymi i chroniących kluczowe aktywa informacyjne organizacji.
- Podsumowanie szkolenia i kanały wsparcia operacyjnego
    - Synteza kluczowych wniosków: Utrwalenie priorytetowych zasad cyberhigieny oraz mechanizmów rozpoznawania zagrożeń omówionych podczas sesji.
    - Dedykowane kanały wsparcia i eskalacji: Wskazanie punktów kontaktowych (Helpdesk / Zespół Bezpieczeństwa) oraz ról odpowiedzialnych za wsparcie merytoryczne i techniczne w sytuacjach podejrzenia incydentu.
    - Walidacja kompetencji i ewaluacja: Przeprowadzenie weryfikacji wiedzy w formie quizu lub ankiety końcowej oraz formalne zamknięcie szkolenia.

Wymagania:

Brak wymagań wstępnych. Szkolenie przeznaczone dla wszystkich pracowników – nie jest wymagana wiedza techniczna ani doświadczenie w obszarze cyberbezpieczeństwa.

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia sygnowany przez Compendium CE (ukończenie szkolenia).

Prowadzący:

Instruktor Compendium Centrum Edukacyjnego.

Informacje dodatkowe:

Pokrycie ustawowego zakresu i odniesienia do przepisów z Nowelizacji Ustawy o KSC:

- Edukacja personelu z zakresu cyberbezpieczeństwa: Art. 8 ust. 1 pkt 2 lit. i.
- Wdrażanie i stosowanie zasad cyberhigieny: Art. 8 ust. 1 pkt 2 lit. j.
- Zapewnienie, aby personel znał wewnętrzne regulacje i obowiązki: Art. 8d pkt 4.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Dla podmiotów publicznych (jeżeli dotyczy): stosowanie zasad cyberhigieny – załącznik nr 4, pkt I ppkt 14; szkolenia osób przetwarzających informacje w zakresie rodzajów zagrożeń, cyberhigieny, reagowania na incydent i skutków naruszeń – załącznik nr 4, pkt I ppkt 17

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001