Koncept školení – Základy kybernetické bezpečnosti

Produkty

- Školení zaměstnanců základů kybernetické bezpečnosti
- Školení pro management základů kybernetické bezpečnosti

Rozsah

- Jednodenní školení – 2 hodiny, pauza a 2 hodiny
- Strukturu jednotlivých školení rozpracovat na 50-60 slide
- Školení zaměstnanců a školení pro managment s cca 50-60 % shodným základem obsahu školení následně rozděleným do dvou větví samostatných témat
- Závěrečný test pro ověření znalostí

Cíle

Úvod do kybernetické bezpečnosti a bezpečnosti informací. Kurz slouží k pochopení řízení informační bezpečnosti a vysvětlení jednotlivých technických nástrojů.

Přínosy

- Porozumění pojmům jako ISMS
- Vysvětlení přínosu technických a organizačních nástrojů
- Techniky a taktiky kybernetického útoku a obrany
- Vysvětlení oblastí jako je 802.1x, BYOD, PAM ad.
- Pochopení cílů bezpečnosti informací a vztahu řízení bezpečnosti informací k zájmům organizace.

Formát školení

Standardně prezenční formou nebo online. Kurz je teoretický se závěrečným vyhodnocením.

Požadavky

Pro toto školení je potřebná základní orientace v ICT prostředí. Pro online výuku vlastní standardní počítačové vybavení s připojením na internet.

Cílová skupina

- Kdokoliv, kdo se v bezpečnosti informací neorientuje a měl by zájem o obecný přehled.
- Zaměstnavatelé, kteří potřebují u managementu a zaměstnanců zvýšit povědomí v oblasti bezpečnosti informací.
- Technické role jiných oblastí ICT za účelem získání základního povědomí o bezpečnosti informací
- Široká veřejnost se zájmem o moderní trendy v bezpečnosti informací

Literatura

Účastníci obdrží přístup k tištěné nebo elektronické verzi studijních materiálů.

Struktura – Školení zaměstnanců

1. **Úvod do školení a kybernetické bezpečnosti**
   a. Ukázka
   b. Historie s časovým vývojem od prvního výskytu až do současnosti
   c. Dopady škod napáchaných bezpečnostními incidenty
      a. Proč je kybernetická bezpečnost důležitá
      b. Threat map
   d. Vnitropodnikové hrozby
2. **Kybernetická bezpečnost**
   a. Co je to kybernetická bezpečnost a čím se zabývá
      a. CIA triády – důvěrnost, integrita a dostupnost
      b. Základní pojmy – identita, aktiva, zranitelnost…
   b. Legislativní rámec
      a. Zákon a vyhláška o kybernetické bezpečnosti
      b. ISMS – Systém řízení bezpečnosti informací
         a. Vymezení ISMS
         b. Organizační opatření
         c. Technická opatření
         d. Bezpečnostní politika a bezpečnostní dokumentace
         e. Kybernetický bezpečnostní incident
         f. Reaktivní opatření
         g. Shrnutí
   c. Instituce a orgány zabývající se kybernetickou bezpečností v ČR
3. **„RED TEAM“ Kybernetický útok**
   a. Klasifikace útočníků a jejich příklady
      a. Hobbyst
      b. Organized crime
      c. Nation-state actors
      d. Hacktivist
      e. Terrorist
   b. Cíle útočníků
      a. Individua
      b. Společnosti
      c. Banky
      d. Vláda
      e. Média
      f. Extrémisti
   b. Formy kybernetických útoků
      a. Malware
      b. Phishing
      c. Craking
      d. SQL Injection a Cross-site scripting
      e. Man-in-the Middle a Hijacking
      f. Sociální inženýrství
      g. Fake advertising
      h. DoS a DDoS email/web server

i. SPAM
j. Injection
k. DNS spoofing
l. Sniffing
m. Cybersquatting
n. Mimicking
o. Kyberterorismus
p. Zero-day

b. Nejčastější zranitelnosti
   a. Validace vstupu
   b. Řízení vstupu
   c. Autentizace
   d. Objetí autorizace
   e. Ošetření chyb
   f. Neověřené zdroje

c. Fáze kybernetického útoku
   a. Identifikace
   b. Přístup
   c. Eskalace
   d. Vytrvalost
   e. Exfiltrace
   f. Útok
   g. Zahlazení

4. **„BLUE TEAM“ Kybernetická obrana**
   a. Přehled bezpečnostních nástrojů a opatření
      a. Rozšiřovaní myšlenky o kybernetické bezpečnosti
      b. Firewall
      c. 802.1x
      d. IPS, IDS
      e. EDR
      f. SSL koncentrátor
      g. Sondy detekce průniku
      h. Antivir
      i. Proxy Servery,
      j. Identity management
      k. MDM
      l. Vulnerability scannery
      m. Bezpečnostní dohled (SIEM a SOC)
      n. SPAM filter
      o. Sandbox
      p. Security patch
      q. Penetrační testy
      r. Vulnerability scanning
      s. Vzdělávání
   b. Reakce kybernetické obrany a průběh
      a. Příprava
      b. Identifikace
      c. Zadržování
      d. Vymýcení

    e. Obnova
    f. Poučení
5. **Rizikové chování**
    a. Surfování na internetu bezpečně
    b. Důvěrné dokumenty
    b. Osobní údaje na internetu
    c. Platby přes internet
    d. Jak poznat důvěryhodný web a online obchodníka
    e. E-mailová komunikace bezpečně
    f. Hesla
    g. Stahování programů
    h. Používání cizích zařízení
    i. Připojení z cizí sítě
    j. Chytrý mobilní telefon
    k. Zálohování a obnova
6. **Rizikové jevy**
    a. Sociální sítě
    b. Sociální bubliny
    c. Netolismus
    d. Počítačové hry
    e. Pornografie
    f. Sexting
    g. Kybergrooming
    h. Kyberstalking
    i. Kyberšikana
    j. Hatespeech
    k. Dezinformace
7. **Závěrečné zhodnocení**
8. **Test a vyhodnocení**

Struktura – Školení pro management

1. **Úvod do školení a kybernetické bezpečnosti**
    b. Ukázka
    c. Historie s časovým vývojem od prvního výskytu až do současnosti
    d. Dopady škod napáchaných bezpečnostními incidenty
        a. Proč je kybernetická bezpečnost důležitá
        b. Threat map
    e. Vnitropodnikové hrozby
2. **Kybernetická bezpečnost**
    b. Co je to kybernetická bezpečnost a čím se zabývá
        a. CIA triády – důvěrnost, integrita a dostupnost
        b. Základní pojmy – identita, aktiva, zranitelnost…
    b. Legislativní rámec
        a. Zákon a vyhláška o kybernetické bezpečnosti
        b. ISMS – Systém řízení bezpečnosti informací
            a. Vymezení ISMS
            b. Organizační opatření
            c. Technická opatření
            d. Bezpečnostní politika a bezpečnostní dokumentace
            e. Kybernetický bezpečnostní incident
            f. Reaktivní opatření
            g. Shrnutí
    d. Instituce a orgány zabývající se kybernetickou bezpečností v ČR
3. **„RED TEAM“ Kybernetický útok**
    b. Klasifikace útočníků a jejich příklady
        a. Hobbyst
        b. Organized crime
        c. Nation-state actors
        d. Hacktivist
        e. Terrorist
    b. Cíle útočníků
        a. Individua
        b. Společnosti
        c. Banky
        d. Vláda
        e. Média
        f. Extrémisti
    c. Formy kybernetických útoků
        a. Malware
        b. Phishing
        c. Craking
        d. SQL Injection a Cross-site scripting
        e. Man-in-the Middle a Hijacking
        f. Sociální inženýrství
        g. Fake advertising
        h. DoS a DDoS email/web server

i. SPAM
j. Injection
k. DNS spoofing
l. Sniffing
m. Cybersquatting
n. Mimicking
o. Kyberterorismus
p. Zero-day

b. Nejčastější zranitelnosti
   a. Validace vstupu
   b. Řízení vstupu
   c. Autentizace
   d. Objetí autorizace
   e. Ošetření chyb
   f. Neověřené zdroje

d. Fáze kybernetického útoku
   a. Identifikace
   b. Přístup
   c. Eskalace
   d. Vytrvalost
   e. Exfiltrace
   f. Útok
   g. Zahlazení

4. **„BLUE TEAM“ Kybernetická obrana**

b. Přehled bezpečnostních nástrojů a opatření
   a. Rozšiřovaní myšlenky o kybernetické bezpečnosti
   b. Firewall
   c. 802.1x
   d. IPS, IDS
   e. EDR
   f. SSL koncentrátor
   g. Sondy detekce průniku
   h. Antivir
   i. Proxy Servery,
   j. Identity management
   k. MDM
   l. Vulnerability scannery
   m. Bezpečnostní dohled (SIEM a SOC)
   n. SPAM filter
   o. Sandbox
   p. Security patch
   q. Penetrační testy
   r. Vulnerability scanning
   s. Vzdělávání

c. Reakce kybernetické obrany a průběh
   a. Příprava
   b. Identifikace
   c. Zadržování
   d. Vymýcení

e. Obnova
f. Poučení

5. **Systém řízení bezpečnosti informací ISMS**
    1. **Organizační opatření**
        a. Systém řízení bezpečnosti informací – ISMS
            a. PDCA cyklus (Plan – Do – Check – Act)
            b. ISO/IEC 27001
            c. Stanovení rozsahu
        b. Řízení aktiv
        c. Řízení rizik
        d. Organizační bezpečnost
        f. Řízení dodavatelů
        g. Bezpečnost lidských zdrojů
        h. Řízení provozu a komunikací
        i. Řízení změn
        j. Řízení přístupu
        k. Akvizice, vývoj a údržba
        l. Zvládání kybernetických bezpečnostních událostí a incidentů
        m. Řízení kontinuity činností
        n. Audit kybernetické bezpečnosti
        o. Fyzická bezpečnost
    2. **Technická opatření**
        1. Bezpečnost komunikačních sítí
        2. Správa a ověřování identit
        3. Řízení přístupových oprávnění
        4. Ochrana před škodlivým kódem
        5. Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
        6. Detekce kybernetických bezpečnostních událostí
        7. Sběr a vyhodnocování kybernetických bezpečnostních událostí
        8. Aplikační bezpečnost
        9. Kryptografické prostředky
        10. Zajišťování úrovně dostupnosti informací
        11. Průmyslové, řídicí a obdobné specifické systémy
        12. Digitální služby
    3. **Bezpečnostní politika a bezpečnostní dokumentace**
    4. **Kybernetický bezpečnostní incident**
    5. **Reaktivní opatření a kontaktní údaje**
6. **Praktická aplikace teoretických znalostí na fiktivní společnosti**
7. **Závěrečné zhodnocení**
8. **Test a vyhodnocení**