ZAKŁAD ROZWOJU TECHNICZNEJ OCHRONY MIENIA TECHOM SP. Z O.O.

Jednostka Certyfikująca
na Znak PN
PN-EN 16763

Al. Wyzwolenia 12, 00-570 Warszawa
tel. (22) 625-34-00, fax (22) 625-26-75
www.techom.com
techom@techom.com

Wpis do KRS Nr 0000164572
NIP: 5260011894
Regon: 010663796

KOD NCAGE **9A57H**

OFERTA SZKOLENIA

SZKOLENIE W ZAKRESIE CYBERBEZPIECZEŃSTWA W SYSTEMACH ZABEZPIECZEŃ TECHNICZNYCH

– forma zdalna

O SZKOLENIU

Szkolenie pokazuje, jak zarządzać cyberbezpieczeństwem systemów zabezpieczeń technicznych (SSWiN, SKD, VSS/CCTV) – od zrozumienia zagrożeń, podatności i technik ataków, przez podstawowe mechanizmy ochrony, bezpieczne protokoły komunikacji oraz zabezpieczenia systemów dozoru wizyjnego, aż po zarządzanie ryzykiem w odniesieniu do międzynarodowych standardów, wymagania prawne oraz planowanie, projektowanie i instalowanie cyberbezpiecznych systemów zabezpieczeń technicznych (secure by design i secure by default).

ZAGROŻENIA I PODATNOŚCI » **MECHANIZMY OCHRONY** » **BEZPIECZNA ARCHITEKTURA I PROTOKOŁY** » **ZARZĄDZANIE RYZYKIEM** » **REAGOWANIE NA INCYDENTY**

ORGANIZACJA SZKOLENIA

TERMIN	Zgodnie z ofertą na stronie.
FORMA	Zdalna w czasie rzeczywistym – MS Teams (zajęcia prowadzone na żywo; link dostępowy uczestnicy otrzymują przed rozpoczęciem szkolenia, dołączenie do spotkania jako gość, bez zakładania konta).
CZAS TRWANIA	3 dni – 19 godzin zegarowych (łącznie z przerwami). Godzina rozpoczęcia: 9.00.
CENA	3150,00 zł netto + 23% VAT od osoby. Możliwość zw. z VAT na podstawie oświadczenia – dotyczy uprawnionych jednostek. Cena obejmuje: szkolenie, materiały dydaktyczne, test, wydanie zaświadczenia o ukończeniu szkolenia.
TERMIN ZGŁOSZEŃ	Do dwóch tygodni przed rozpoczęciem szkolenia (po tym terminie zgłoszenia będą przyjmowane warunkowo).

DLA KOGO JEST TO SZKOLENIE?

- projektanci, instalatorzy, administratorzy oraz integratorzy systemów zabezpieczeń technicznych, w szczególności systemów CCTV/VSS, SSWiN, SKD oraz innych systemów ochrony technicznej,
- specjaliści odpowiedzialni za nadzór nad bezpieczeństwem i odpornością systemów zabezpieczeń technicznych,
- osoby planujące i realizujące inwestycje w systemy zabezpieczeń technicznych po stronie inwestora lub zamawiającego, w tym definiujące wymagania bezpieczeństwa oraz nadzorujące ich wdrożenie,
- specjaliści ds. bezpieczeństwa IT/OT zaangażowani w integrację systemów zabezpieczeń technicznych z infrastrukturą teleinformatyczną oraz w zapewnienie ich bezpiecznej eksploatacji,
- przedstawiciele producentów i dystrybutorów rozwiązań w obszarze systemów zabezpieczeń technicznych odpowiedzialni za rozwój, wdrażanie i wsparcie technologiczne oferowanych systemów,
- osoby odpowiedzialne za zarządzanie bezpieczeństwem obiektów, w tym obiektów o podwyższonych wymaganiach w zakresie ochrony.

DOKUMENTY PO SZKOLENIU

Szkolenie kończy się testem sprawdzającym wiedzę (walidacja: test teoretyczny – pisemny); uczestnicy otrzymują **zaświadczenie o ukończeniu szkolenia.**

KONTEKST PRAWNY I NORMATYWNY

Ustawa o Krajowym Systemie Cyberbezpieczeństwa wymagania przepisów w zakresie cyberbezpieczeństwa	**Ustawa o zarządzaniu kryzysowym** powiązanie z wymaganiami ustawy o KSC; dostawcy wysokiego ryzyka z perspektywy rynku systemów zabezpieczeń technicznych; wymagania w zakresie cyberbezpieczeństwa dla infrastruktury krytycznej	**PN-EN ISO/IEC 27001:2023-08** Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Systemy zarządzania bezpieczeństwem informacji – Wymagania

TEMATYKA SZKOLENIA

Blok 1: Fundamenty cyberbezpieczeństwa i kontekst prawno-normatywny

- wprowadzenie do cyberbezpieczeństwa systemów zabezpieczeń technicznych: podstawowe pojęcia (zagrożenia, podatności, ataki, ochrona); znaczenie cyberbezpieczeństwa w systemach bezpieczeństwa fizycznego (SSWiN, SKD, VSS/CCTV);
- bezpieczeństwo cybernetyczne – jaki mamy problem? Realia doby komunikacji globalnej; urządzenia i technologie „smart" oraz IoT; główne podmioty w sferze bezpieczeństwa cybernetycznego; case study – przykłady naruszeń; ryzyko a zagrożenie;

- problem bezpieczeństwa cybernetycznego „od kuchni": czynnik ludzki; architektura współczesnych systemów zabezpieczeń technicznych; inżynieria oprogramowania i błędy; podstawowe zasady bezpieczeństwa; bezpieczeństwo fizyczne, komputerów i urządzeń mobilnych;
- podstawy cyberbezpieczeństwa: podstawowe zagrożenia i ataki (malware, ransomware, phishing, DDoS); najczęściej stosowane techniki ataków, podatności i backdoor, ataki socjotechniczne; podstawowe mechanizmy ochrony (firewall, IDS/IPS); podstawy kryptografii;
- incydenty: rodzaje incydentów, zgłaszanie, obsługa wewnątrz organizacji, analiza powłamaniowa; systemy chmurowe – wyzwania otoczenia chmurowego, modele usług i modele wdrożeniowe;
- kontekst prawno-normatywny cyberbezpieczeństwa. Wymagania przepisów ustawy o Krajowym Systemie Cyberbezpieczeństwa i ich powiązanie z założeniami projektu nowelizacji ustawy o zarządzaniu kryzysowym. Dostawcy wysokiego ryzyka z perspektywy rynku systemów zabezpieczeń technicznych.

Blok 2: Cyberbezpieczeństwo systemów dozoru wizyjnego

- wprowadzenie do cyberbezpieczeństwa systemów dozoru wizyjnego: potencjalne zagrożenia dla sieci monitoringu wizyjnego; typowe ataki i ich wpływ na systemy VSS/CCTV;
- wybór bezpiecznych protokołów komunikacji i integracji: przegląd protokołów sieciowych; implementacja HTTPS i TLS; protokoły szyfrowane i nieszyfrowane; standardy i zgodność;
- rozwiązania minimalizujące ryzyko naruszeń bezpieczeństwa: firewall, segmentacja sieci i VLAN, autoryzacja, regularne audyty bezpieczeństwa, szkolenie personelu; narzędzia do monitorowania systemów bezpieczeństwa, analiza logów i alertów, automatyzacja zadań bezpieczeństwa, integracja z systemami bezpieczeństwa fizycznego;
- zabezpieczenia systemów dozoru wizyjnego: zarządzanie hasłami, użytkownikami i dostępem zdalnym; regularna aktualizacja oprogramowania; certyfikaty i szyfrowanie; zarządzanie portami i filtrowanie IP; wyłączanie nieużywanych funkcji; bezpieczeństwo na poziomie sieci (802.1x); strategia warstwowa bezpieczeństwa; monitoring i analiza logów.

Blok 3: Zarządzanie ryzykiem i projektowanie cyberbezpiecznych systemów

- rola projektanta systemów bezpieczeństwa: relacje między konsultantami a integratorami; identyfikacja elementów dokumentacji projektowej odpowiedzialnych za cyberbezpieczeństwo;
- PN-EN ISO/IEC 27001:2023-08 jako narzędzie w zarządzaniu bezpieczeństwem: zarys normy; cykl Deminga i system zarządzania bezpieczeństwem informacji; przykłady praktycznej implementacji w systemach zabezpieczeń technicznych; aspekt audytowania;
- podstawy zarządzania ryzykiem dla systemów zabezpieczeń w odniesieniu do międzynarodowych standardów: akty prawne, analiza i szacowanie ryzyka, aktywa i zasoby, zagrożenia i podatności; bezpieczeństwo produktów i danych; publiczne bazy podatności; badanie bezpieczeństwa i testy penetracyjne;
- architektura cyberbezpieczeństwa systemów zabezpieczeń technicznych – secure by design i secure by default; planowanie, projektowanie i instalowanie cyberbezpiecznych systemów zabezpieczeń technicznych; dobre praktyki.

EFEKTY UCZENIA SIĘ

Absolwent szkolenia:

1. charakteryzuje podstawowe pojęcia z zakresu cyberbezpieczeństwa systemów zabezpieczeń technicznych;
2. identyfikuje podstawowe wymagania systemu zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001 w kontekście systemów zabezpieczeń technicznych;
3. identyfikuje podstawowe wymagania prawne w zakresie cyberbezpieczeństwa;
4. identyfikuje podstawowe mechanizmy techniczne funkcjonowania systemu cyberbezpieczeństwa w systemach zabezpieczeń technicznych;
5. charakteryzuje rozwiązania bezpieczeństwa sieciowego dla systemów zabezpieczeń technicznych;
6. ocenia ryzyko cyberbezpieczeństwa w systemach zabezpieczeń technicznych w oparciu o analizę aktywów, zagrożeń i podatności;
7. analizuje zagrożenia i scenariusze ataków na systemy zabezpieczeń technicznych;
8. rozróżnia zdarzenia i incydenty cyberbezpieczeństwa w systemach zabezpieczeń technicznych oraz identyfikuje podstawowe zasady reagowania;
9. identyfikuje podstawowe metody oceny bezpieczeństwa systemów zabezpieczeń technicznych;
10. analizuje zagrożenia i incydenty cyberbezpieczeństwa w systemach zabezpieczeń technicznych oraz wykorzystuje dostępne informacje do podejmowania decyzji projektowych i eksploatacyjnych.

Walidacja: osiągnięcie efektów uczenia się jest weryfikowane podczas walidacji końcowej – test teoretyczny (pisemny).

WARUNKI UCZESTNICTWA

Wymagania techniczne (forma zdalna): komputer z systemem Windows 7 lub nowszym; łącze min. 10 Mbit/s (pobieranie) i 2 Mbit/s (wysyłanie); sprawne słuchawki lub głośniki, mikrofon oraz kamera; zainstalowana aplikacja Microsoft Teams (uczestnik dołącza do spotkania jako gość, bez zakładania konta).

ZGŁOSZENIE NA SZKOLENIE

1. Pobierz i wypełnij kartę zgłoszenia (zgodę dotyczącą przetwarzania danych osobowych podpisuje bezpośrednio uczestnik).
2. Opłać szkolenie – nr konta: 60 1240 6218 1111 0000 4615 3700 (instytucje państwowe i spółki Skarbu Państwa mogą dokonać opłaty po zrealizowaniu szkolenia).
3. Prześlij skan podpisanej karty zgłoszenia (może być podpisana podpisem kwalifikowanym lub przez ePUAP) oraz potwierdzenie przelewu na adres techom@techom.com.
4. Oczekuj potwierdzenia przyjęcia zgłoszenia i szczegółów organizacyjnych.

Kontakt: tel. 22 625 34 00 lub 797-627-524, e-mail: techom@techom.com, www.techom.com.

Wykładowcami będą znani i cenieni specjaliści ds. cyberbezpieczeństwa, w tym byli i obecni kierownicy komórek odpowiedzialnych za cyberbezpieczeństwo w administracji rządowej i instytucjach infrastruktury krytycznej, specjaliści ds. bezpieczeństwa sieci, specjaliści w zakresie testów penetracyjnych oraz rzeczoznawcy ds. systemów zabezpieczeń technicznych.

Organizator szkolenia zastrzega sobie prawo do zmian w planie szkolenia zgodnie z występującymi potrzebami w tym zakresie. Ostateczny plan szkolenia uczestnicy otrzymają w pierwszym dniu szkolenia, przed jego rozpoczęciem. Organizator zastrzega również prawo do zmiany planu szkolenia w trakcie jego trwania.