Konferencja naukowa
„Wzmacnianie odporności szkół wyższych
na cyberataki przez podnoszenie kompetencji cyfrowych”

Czy uczelnie wyższe potrzebują SOC?

Prelegent:Przemysław Dęba

Ministerstwo Edukacji i Nauki

UKSW Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

CLTC Centrum Liderów Transformacji Cyfrowej

Incydenty teleinformatyczne – integralna część świata IT

- Ataki są liczniejsze, bardziej zróżnicowane i bardziej destrukcyjne
- Nie ma 100% bezpieczeństwa, więc trzeba być przygotowanym
- Czas wykrywania, reagowania i przywracania jest krytyczny – ciągłość
- Brak referencji i jednoznacznych definicji
- Im bardziej liberalne polityki i mniej prewencji tym więcej incydentów

Incydenty na uczelniach (AGH projekt SOCCER)

- Przejęcia danych logowania do poczty
- Podejrzana aktywność użytkownika (logowania z krajów wysokiego ryzyka)
- Włamania na strony i serwery jednostek, konferencji, kół naukowych
- Lokalne infekcje ransomware
- Wycieki danych logowania
- Phishing
- Podatności

Gdzie sięgać ?

- NIST SP 800-61
- ISO/IEC 27035

- GIAC Certified Incident Handler (GCIH)
- EC-Council’s Certified Incident Handler (E|CIH)
- Incident Handling & Response Professional (IHRP)
- Certified Computer Security Incident Handler (CSIH)
- Certified Incident Handling Engineer (CIHE)

Zasady, plany i procedury

- Wprowadzone decyzją ścisłego kierownictwa
- Zakres i cele
- Definicje incydentu i pochodnych
- Struktura organizacyjna, role, odpowiedzialności, poziomy eskalacji
- Zasady komunikacji i współdzielenia informacji
- Priorytetyzacja
- Mierniki efektywności
- Raportowanie i wzorce dokumentów
- Roadmapa rozwoju
- Standardowe procedury operacyjne

c

Modele zespołu

Sposób działania

Centralny	Mniejsze organizacje, mała różnorodność geograficzna
Rozproszony	Duże rozproszone organizacje, powinny być koordynowane
Koordynujący	Koordynacja i wsparcie bez ponoszenia odpowiedzialności

Rodzaj zatrudnienia

Pracownicy	W pełni samodzielny z ograniczonym wsparciem dostawców
Częściowy outsource	Wyodrębnienie części zespołu np. 24h monitoring lub 3L ekspercka
Pełny outsource	Zwykle on-site w przypadku braku własnych kompetencji

Wybór modelu

- Dostępność 24h jest pożądana, ze względu na czas trwania incydentu i współpracę z innymi podmiotami
- W przypadku braku dedykowanego zespołu czasami stosuje się model zespołu wirtualnego typu „ochotnicza straż pożarna”
- Odpowiednia struktura i podział ról podnosi morale zespołu
- Konieczna szeroka i uzupełniana wiedza jest obok dostępności 24h głównym czynnikiem kosztotwórczym
- Znajomość organizacji vs specjalistyczne umiejętności i możliwość korelowania zdarzeń
- Plany rozwoju zespołu determinują jego skalowalność
- Delegowanie odpowiedzialności i poufność danych
- Obecność on-site może być konieczna

Struktura i otoczenie zespołu

SOC Monitoring	
Incidents Handlers	
Malware Investigators	PR&Communication
Digital Forensics	Risk Management
Threat Intelligence Team	HR
Security Engineers	Legal
IT admins and support	Branding
Pen Testers	Auditors
	Loss Prevention
	Physical Security

Główne rekomendacje

- Liczbę incydentów zmniejszać można poprzez stosowanie prewencji
- Procedura reagowania, a zwłaszcza interakcje z zewnętrznymi podmiotami powinna być przygotowana wcześniej i udokumentowana
- Warto skupić się na typowych wektorach ataków
- W detekcji ważna jest jakość źródeł danych i poziom automatyzacji
- Priorytetyzacja alertów jest krytycznym punktem decyzyjnym
- Analizy pozdarzeniowe są potężnym narzędziem korygującym

Dziękuję za uwagę