12 - LEGAL DEFENSE, DAMAGE, REGRESS

Cel dokumentu

Ten dokument porządkuje granice legalnej cyberobrony, ścieżkę dokumentowania szkód, zasady przypisywania odpowiedzialności oraz mechanizm regresu i naprawy strat.

Pozycja w architekturze CST

/Common-Source-of-Truth/legal
/Common-Source-of-Truth/legal/defense-rules
/Common-Source-of-Truth/damage-regress
/Common-Source-of-Truth/evidence/chain-of-custody

Defensywa rekomendowana

Dozwolona i rekomendowana defensywa obejmuje monitoring własnych systemów, wykrywanie incydentów, blokowanie złośliwego ruchu, izolację hostów, zabezpieczanie dowodów, zgłaszanie incydentów, MFA, patch management, backup, hardening, threat intelligence, szkolenia i testy bezpieczeństwa za zgodą.

Legalna ofensywa

Legalna ofensywa oznacza działania zgodne z prawem, bez włamywania się do cudzych systemów i bez odwetu. Obejmuje analizę źródeł, IoC, infrastruktury atakujących, takedown przez zgłoszenie domen/hostingu/profili, red teaming wyłącznie na podstawie pisemnej zgody, honeypot we własnej infrastrukturze, legalny sinkholing z właściwymi partnerami, zawiadomienia, roszczenia, blokady we własnych systemach, dowody oraz współpracę z operatorami, hostingiem, platformami i organami.

Niedozwolone działania

- hack-back,
- przejmowanie cudzych kont,
- włamania do infrastruktury sprawcy,
- publikowanie danych osobowych podejrzanych,
- samodzielne karanie sprawców,
- podszywanie się pod organy,
- nieautoryzowane testy cudzych systemów.

Model dochodzenia naprawienia szkód

K0NSULT może przygotowywać materiał do wezwania do zaprzestania naruszeń, zgłoszenia do CERT/CSIRT, zawiadomienia organów ścigania, zgłoszenia do regulatora, roszczenia cywilnego, zgłoszenia do ubezpieczyciela, postępowania administracyjnego i raportu dla poszkodowanych.

Tabela obciążania szkód

Pole	Opis
ID szkody	kod szkody
ID incydentu	powiązanie
Poszkodowany	osoba / podmiot
Sprawca	A0-A5
Poziom pewności	hipoteza / techniczny / wysoki / legalny
Wartość szkody	kwota
Dowód szkody	faktura, log, koszt pracy, raport

Pole	Opis
Podstawa roszczenia	cywilna, karna, administracyjna
Organ/ścieżka	policja, sąd, regulator, ubezpieczyciel
Status	analiza / zgłoszone / w toku / odzyskane / umorzone
Kwota odzyskana	wartość
Kwota nieodzyskana	wartość

Panel nadzorczy

Poziom	Widok
Strategiczny	bezpieczeństwo państwa/jednostki, trendy, BigTech
Operacyjny	aktywne incydenty, priorytety, właściciele
Techniczny	logi, systemy, podatności, IoC
Dowodowy	dowody, hashe, chain of custody
Prawny	AI Act, NIS2, RODO, KSC, organy
Finansowy	szkody, koszty, naprawa strat
Szkoleniowy	operatorzy, certyfikaty, ćwiczenia
Rozwojowy	własne technologie, skalowanie, roadmapa

Zasada odpowiedzialności

Nie przypisywać winy bez dowodu. Nie mylić źródła technicznego z osobą odpowiedzialną. Nie publikować danych osób bez podstawy prawnej. Każdy claim musi mieć źródło, każdy dowód status, a każde działanie właściciela.