Incident Response
Takeaway from the field

Roberto Caramia, Head of Incident Response CSIRT Italia

Turin, 25.05.2022

The Four Basic Pillars of the Italian Cybersecurity Architecture

CYBERSECURITY

Cyber Resilience	Cyber Investigation	Cyber Defence	Cyber Intelligence
AGENZIA PER LA CYBERSICUREZZA NAZIONALE – ACN – SAPIENTIA ADIUVAT CSIRT Italia – Computer Security Incident Response Team	- National Police - Carabinieri - Financial Guard	- Military Defence	- DIS - AISE - AISI

SYNERGIES

SYNERGIES

ACN's «*Operations*» Service Functions

Incident Handling & Response

Incident Handling Support

Remediation Plan Definition Support

Malware and Suspicious Artefact Analysis

Digital Forensics & «Post-Mortem» Analysis

Threat Intelligence

Exposed Attack Surface Monitoring

Actors, Campaigns & Vulnerability Monitoring

Expert analysis on cyber threats

Early Warning on Events of National Relevance

Risk Management & Compliance

Incident Systemic Impact Evaluation

Vulnerability Systemic Impact Evaluation

Forecast Analysis and Threat Trends

Frameworks & Standards Compliance

Obiettivi dell' Incident Response

Investigate

- Determinare il vettore di attacco
- Determinare i tool ed il malware utilizzato
- Identificare i sistemi compromessi e le modalità di compromissione
- Determinare la profondità della compromissione e eventuali impatti sulla confidenzialità dei dati gestiti
- Determinare se l'incidente è ancora in corso
- Identificare la timeline dell'incidente

Remediate

Utilizzare le informazioni raccolte per definire ed eseguire il piano di rimedio

Don't Act too Quickly

Neither too slow…

Takeaway

Fattori di rischio

- Iniziare il processo di remediation senza avere abbastanza elementi espone a maggiori rischi
- L'attaccante potrebbe identificare le azioni di remediation ed intensificare le attività di persistenza o effettuare azioni distruttive
- Ripristinare immediatamente i sistemi senza le corrette informazioni può generare impatti imprevisti ed esporre l'infrastruttura a maggiori rischi
- Effettuare attività invasive o di ripristino immediato potrebbe portare alla distruzione di evidenze fondamentali

Don't be an ostrich

Takeaway

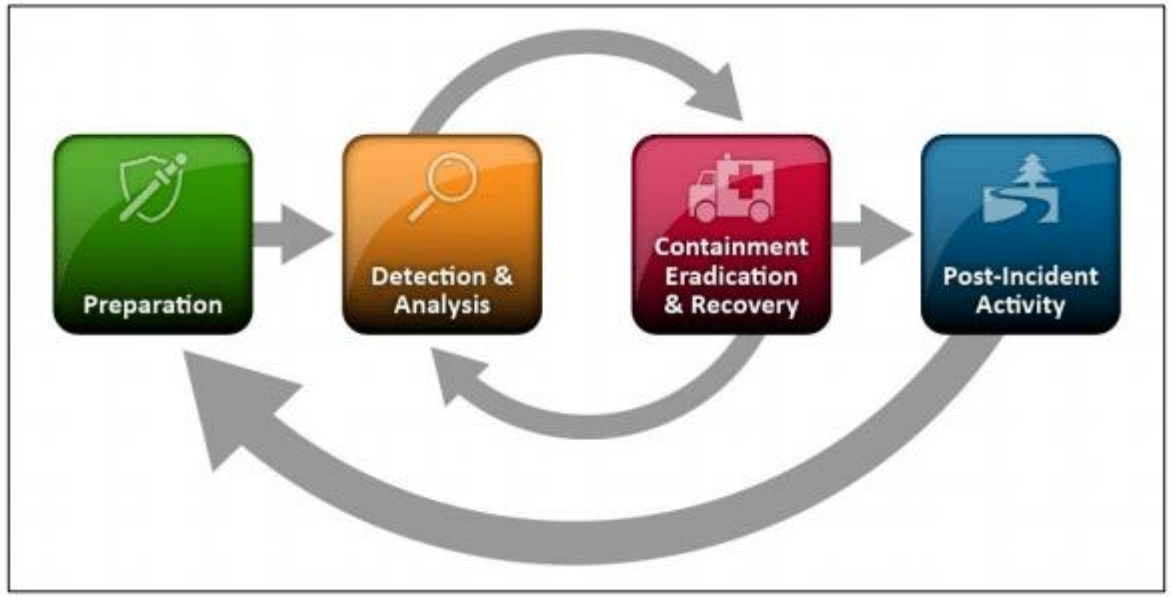
Attività di comunicazione

- Provare a nascondere o minimizzare un incidente può comportare un maggiore impatto sia dal punto di vista mediatico sia dal punto di vista operativo
- Segnalare un incidente agli organi preposti oltre a scongiurare la possibilità di incappare in regimi sanzionatori consente di ottenere supporto e di proteggere la comunità nazionale
- Una comunicazione efficace interna ed esterna all'organizzazione consente di prevenire ulteriori danni d'immagine di agevolare le attività del team di risposta

Follow a structured approach to IR

Takeaway

Processo di Incident Response



Source NIST

Know your environment

Takeaway

Preparation

- Mantenere aggiornato l'asset management
- Categorizzare i sistemi ed i dati utilizzati in base alle loro funzioni e criticità
- Identificare e mantenere una lista degli stakeholder (ruoli/responsabilità/contatti) interni ed esterni all'organizzazione
- Formare il personale a tutti i livelli sui rischi legati alla sicurezza informatica sulle buone pratiche da adottare e sulle procedure di risposta agli incidenti informatici
- Attivare il Team di risposta (IR-TEAM) coinvolgendo tutti gli attori necessari interni/esterni tecnici/decisionali amministrativi/legali

Get visibility and stay focused

Takeaway

Detection & Analysis

- Mantenere la più ampia visibilità su tutto l'ambiente da proteggere (EDR/XDR/SIEM/SOAR/TI…)
- Definire una baseline di funzionamento dei propri sistemi
- Monitorare costantemente il proprio ambiente alla ricerca di anomalie
- Prioritizzare l'analisi delle anomalie rilevate in base alla categorizzazione degli asset
- Approfondire qualsiasi comportamento, informazione o segnalazione ricevuta che possa rappresentare un precursore o un indicatore di incidente

Observe, Orient, Decide, Act

Takeaway

Containment Eradication & Recovery

- Limitare le capacità dell'attaccante per prevenire ulteriori impatti mantenendo attive le funzioni essenziali
- Identificare e bloccare i canali di comando e controllo dell'attaccante
- Identificare e rimediare le ulteriori vie d'accesso presenti nella rete (es. vulnerabilità misconfigurazione utenze dormienti)
- Identificare e «bonificare» tutti gli asset compromessi/utilizzati dall'attaccante
- Ripristinare tutti i servizi affetti prendendo tutte le misure necessarie per evitarne la recompromissione
- Documentare tutte le evidenze rilevate e le attività effettuate in dettaglio

Learn from the incident and plan for the future

Takeaway

Post-incident Activity

- Valutare l'efficacia dei processi di gestione dell'incidente implementati e revisionarli in base all'esperienza acquisita
- Identificare i gap capacitivi e di processo che hanno facilitato/consentito l'incidente
- Avviare un processo continuo di revisione della postura e delle procedure operative adottate

Grazie


AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT