Security operation gestione degli incidenti

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Security operation gestione degli incidenti

- Dal monitoraggio all'intrusion prevention
- Gestione degli incidenti (Damage Control)

..

Systems & Networks Monitoring

Necessario per garantire e controllare la disponibilità dei dati.
Da non sottovalutare la sua funzione in chiave di identificazione di compromissioni della sicurezza.
E' necessario stabilire una baseline affidabile, poi ...

- Un server sta facendo traffico anomalo?
- Un client cerca di collegarsi ad altri client?
- Un client produce una quantità di traffico anomalo?
- Un utente crea numerose sessioni da/verso Internet?
- Un'applicazione varia il pattern delle sue transazioni?
- Una linea si satura improvvisamente?

Estremamente efficace nelle situazioni che richiedono una mente umana e non un algoritmo (ma vedi dopo SIEM).
Ovviamente non è semplice quanto sembra!

Intrusion Detection

- Host-based
- Network-based
- Statistical detection
- Pattern-matching detection
- Offline or online analytics

http://en.wikipedia.org/wiki/Intrusion_detection_system

Con Intrusion Detection si identificano metodologie e tecniche per scoprire attività anomale, scorrette o non appropriate nei sistemi e nelle reti.
Host-based, Network-based.
Statistical detection, pattern-matching detection, offline or online analytics.
E' necessario avere una baseline di cosa è “normale” sia sulla rete che sui server.
Autoapprendimento.
Facile avere falsi positivi o mancati rilevamenti.

Network-based IDS

Catturano il traffico che passa sulla rete.
Filtro di primo livello --> estrae il traffico da analizzare, con regole o campionamento
Secondo livello --> analizzatore (pattern matching o statistical: identifica anomalie e frequenza delle stesse)
Terzo livello --> modulo di intervento (logging, alerting)
Il traffico viene catturato tramite un adattatore di rete configurato in Promiscuous Mode (shared media) oppure collegato ad una porta di mirroring dello switch.

Dal monitoraggio all'intrusion prevention

Snort https://www.snort.org/
Suricata https://suricata-ids.org/
NIDS molto leggeri Open Source
Effettuano analisi e logging del traffico IP in tempo reale.
Hanno tre modi: sniffer, logger o NIDS.
L'analisi si basa sulla tecnica del pattern matching.
Quando analizza un pacchetto contenente certi pattern specificati nelle sue regole esegue l'azione ad essi associata (logging, alert…).

Host-based IDS

Fanno un auditing sistematico dei log di sistema e del filesystem.
Real-time vs scheduled auditing.
Tracciano I/O, Process, Port e Network activity.
Modulo di analisi, modulo di intervento.
I più sofisticati si agganciano oppure intercettano direttamente gli hook di sistema.

Debolezze
Intrusion Detection

Debolezze dell'Intrusion Detection

Nel tempo gli IDS si sono rivelati poco utilizzabili.

- NIDS sono come dei guardiani all'ingresso di una Banca cui è consegnato un pacco di fotografie di delinquenti: quando ne vedono uno suonano l'allarme ma lo lasciano entrare
- HIDS sono come guardiani all'interno del caveau della Banca, che controllano che il contenuto sia ancora lì, se sparisce suonano l'allarme (ma intanto è sparito)

Il danno non si può evitare, finché non si dotano i guardiani di strumenti per impedire l'intrusione.

Intrusion Prevention

- Network-based
- Wireless
- Network behavior analysis
- Host-based

http://en.wikipedia.org/wiki/Intrusion_prevention_system

Network-based intrusion prevention system (NIPS)
Wireless intrusion prevention systems (WIPS)
Network behavior analysis (NBA)
Host-based intrusion prevention system (HIPS)
Prima Detection poi Prevention (blocco delle porte sugli apparati di rete, blocco dei MAC Address, kill di processi, spostamento del traffico su LAN isolate ecc.).
Nascono grazie all'aumento della potenza di calcolo di apparati e server.
Esempio: sistema antivirus enterprise

Gestione dei log

http://en.wikipedia.org/wiki/Log_management
Spesso è l'elemento chiave per capire “cosa è successo?” oppure “cosa sta succedendo?”.
Raccolta dei log da vari sistemi chiave con aggregazione centralizzata (timestamp!).

- Per quanto tempo li tengo ?
- Debbo nasconderli agli utenti (privacy)
- Debbo proteggerli dagli attaccanti
- Debbo ruotarli
- Mi servono strumenti di analisi (in tempo reale o a posteriori)
- Mi serve una baseline (“che cosa è normale che ci sia nei miei log ?”)
- Mi servono strumenti di aggregazione e reporting

Insomma, non è semplice quanto sembra !
https://www.splunk.com/

Dal monitoraggio all'intrusion prevention

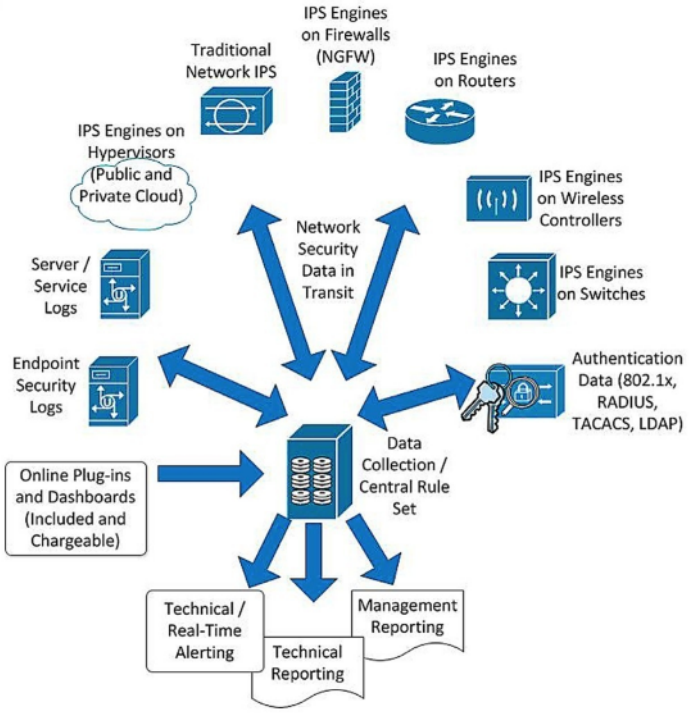
SIEM
Security Information & Event Management

https://en.wikipedia.org/wiki/Security_information_and_event_management

Unisce IPS+gestione dei log+logica:

- Data aggregation
- Correlation
- Alerting
- Dashboards
- Compliance (ad esempio amministratori di sistema)
- Retention
- Forensic analysis

Dal monitoraggio all'intrusion prevention



Si tende ad un modello unico di controllo e di gestione della sicurezza.

Damage Control

E durante l'attacco cosa faccio?

Se sono sotto attacco intendo

Damage Control

E durante l'attacco cosa faccio?

E durante l'attacco cosa faccio?
"Damage control" (termine di derivazione navale che vuol dire: "darsi da fare per non far affondare la nave che imbarca acqua").

- Mettere in sicurezza i dati
- Fare la conta dei danni
- Pianificare azioni di ripristino
- Comunicare (interno, esterno, clienti, fornitori, stakeholders)
- Capire come è successo e di conseguenza attrezzarsi in modo che non succeda più

Damage Control

Israel Defense Forces
@IDF
Segui

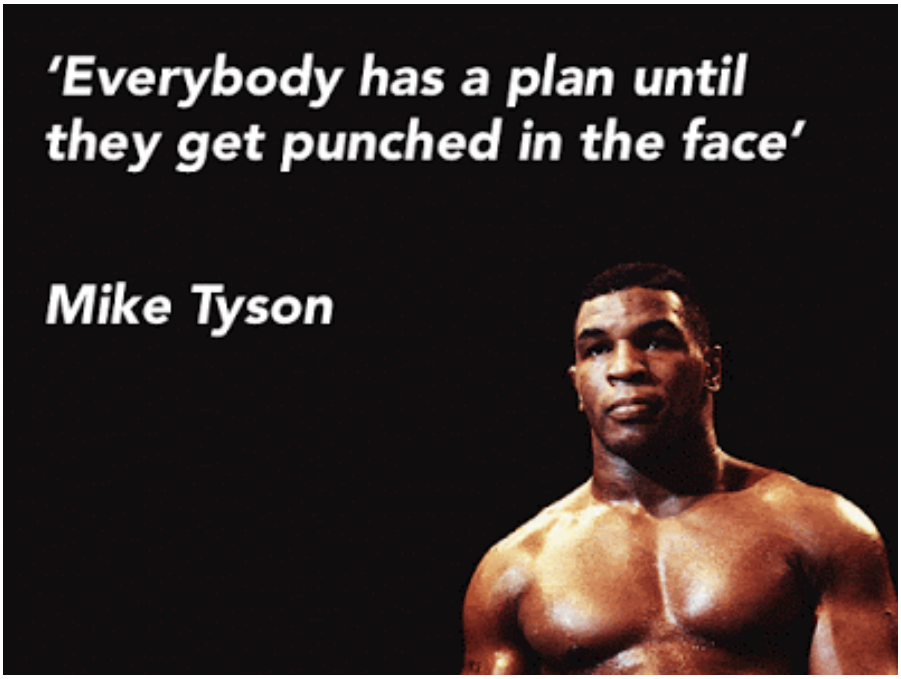
CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work.

HamasCyberHQ.exe has been removed.

Traduci il Tweet

Contrattaccare è illegale.
(anche lanciare missili contro il datacenter dell'attaccante sarebbe da evitare)

Damage Control



Bisogna essere preparati al peggio.

Damage Control

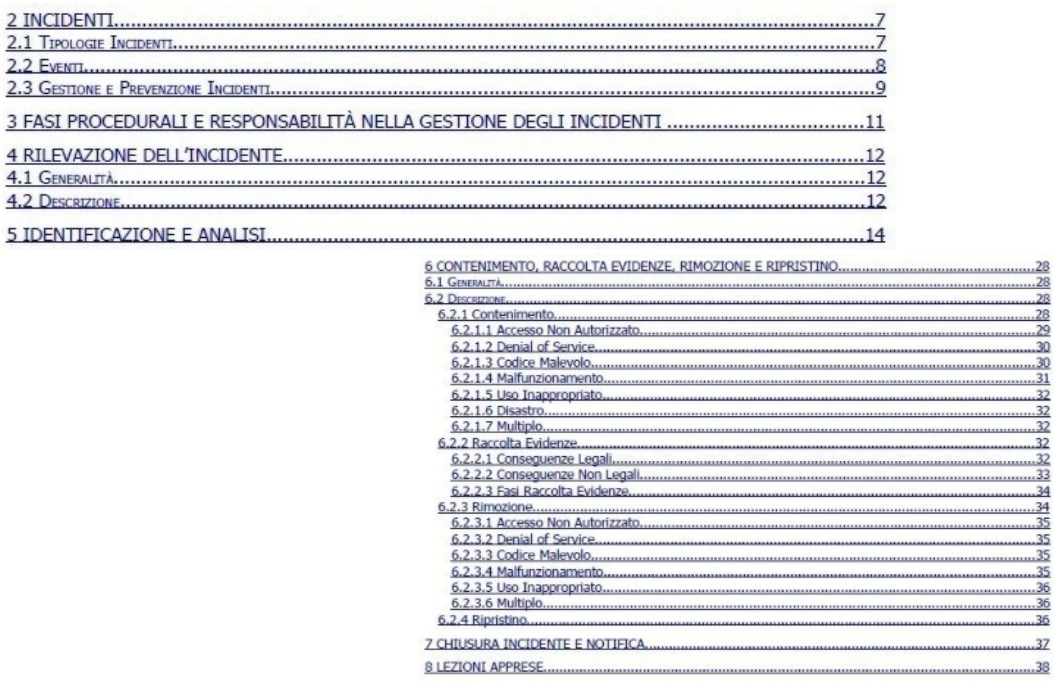
Piano per la gestione degli incidenti informatici

(aggiornato, conosciuto, accessibile, condiviso, unico ...)

Avere un responsabile del piano (o una gerarchia).
Elencare i rischi, le minacce e i potenziali incidenti.
Sviluppare guide rapide per gli scenari più probabili.
Stabilire procedure per prendere le decisioni più importanti.
Modalità di rapporto con i principali interlocutori esterni.
Avere contratti di servizio e con fornitori ed esperti.
Tenere aggiornata e disponibile la documentazione.
Assicurarsi che tutti abbiano chiari i propri ruoli e responsabilità.
Identificare gli individui che sono fondamentali per la risposta agli incidenti e garantire la ridondanza.
Fare simulazioni di incidente e raffinare i piani di conseguenza.

Attenzione! Con la nuova normativa Europea diventa obbligatorio averlo. Segnalare incidente entro 72 ore se coinvolge dati personali.

Damage Control



Disciplinare tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna

Damage Control

Incident Response Team

- IT and security teams
- Outside consultants
- Executive management
- Compliance/Legal
- Business operations
- Human resources
- Public relations/External Communication
- Vendors/Business partners

- IT and security teams
- Outside consultants: se serve competenza extra
- Executive management: per prendere decisioni strategiche (spengo la produzione per x minuti)
- Compliance/Legal (GDPR, eventuali certificazioni, rischi legali del data breach per l'azienda, rischi di azioni da intraprendere)
- Business operations (chiudo il portale ordini, comunicare in azienda)
- Human resources (mi serve quella persona che lavori tutta la notte, comunicazione in azienda, violazione policy)
- Public relations (comunicazione all'esterno, **le parole della crisi (esempio FFSS e il treno "sviato" a Pioltello)**)
- Vendors Business partners (ISP, hw e SW vendor, app vendor ecc.)

Damage Control

Honeypots

https://en.wikipedia.org/wiki/Honeypot_(computing)

Honeypot: vaso di miele per attirare gli attaccanti, può servire per studiare gli attacchi oppure per distrarre l'attaccante. Ambienti simili alla produzione ma innocui e isolati. Es. Caselle di posta predisposte per attirare lo spam. Si può valutare un attacco in corso

By aussiegall from sydney, Australia (Old Honey Pot) [CC BY 2.0 (http://creativecommons.org/licenses/by/2.0)], via Wikimedia Commons

Damage Control

Sandbox

https://en.wikipedia.org/wiki/Sandbox_(computer_security)

Sandbox: buca di sabbia dove far esplodere le bombe. In input ci appoggio le mail sospette prima di recapitarle al destinatario e simulo le azioni che farebbe l'utente per vedere cosa succede (se esplode). Se uso personal mail mi serve una personal sandbox.

In uscita (proxy navigazione) posso testare i link dubbi e vedere cosa fanno (rallenta la navigazione).

Damage Control

Canary

https://canary.tools/

Canary: appliance che fanno scattare allarme quando sono compromesse. No analisi, solo allarme. Più semplice da gestire di Honeypot. (canarini nelle miniere)

http://docs.opencanary.org/ (open source)

Fino a veri e propri sistemi di emulazione di reti aziendali in grado di gestire trappole complesse:
https://en.wikipedia.org/wiki/Deception_technology
Nova (open source) http://www.projectnova.org genera reti e host fittizzi che fanno perdere tempo all'attaccante.

Sono tutti elementi di difesa attiva (legale, contrattacco=illegale)