Questionario sulla cybersecurity

Luca G. Carbone

Tutorial Days CCR 10-12/10/2022 – LNF

Utilizzate uno strumento per la registrazione in tempo reale e la memorizzazione a lungo termine delle associazioni mac address/IPv4 address/IPv6 address (dove applicabile)? Lo strumento è in grado di segnalare in tempo reale l'eventuale duplicazione di un indirizzo IP?

Solo due sezioni su 20 non utilizzano strumenti dedicati al controllo degli indirizzi MAC/IPv4 – lo strumento più diffuso è *arpwatch*, il che implica che non vengano intercetatti gli indirizzi IPv6 (attiva per default con indirizzi link local su quasi tutto da anni), e che quindi in previsione futura i sistemi vadano aggiornati. Non mancano strumenti realizzati in casa, ma la metà della sezioni non implementa la segnalazione automatica di duplicazioni o anomalie.

Utilizzate uno strumento per la rilevazione in tempo reale della topologia di rete a livello 2 e per la rilevazione in tempo reale e la memorizzazione a lungo termine delle associazioni mac address/switch port? Lo strumento è in grado produrre una weather map della rete on-the-fly e di individuare/tracciare eventuali pattern di traffico anomali sino alla sorgente o alla destinazione?

Più della metà delle sezioni non dispone di uno strumento:

- per la ricostruzione automatica della topologia della rete locale
- per la visualizzazione di una weather-map della rete
- per la memorizzazione a breve e lungo termine delle associazioni MAC address/switch port (dove si trova la macchina che produce traffico malevolo/scarica film/…?)

Questo è forse il punto su cui vale la pena di produrre uno sforzo di ricerca tecnologica e standardizzazione.

Utilizzate uno strumento (o una suite di strumenti) per la collezione centralizzata, la memorizzazione, l'analisi dei log di sistema e la correlazione di eventi security related?

Quasi tutti implementano la collezione centralizzata e la memorizzazione dei log (sappiamo da fonte affidabile che stanno aumentando le infrastrutture per la conservazione off-line), quasi nessuno dispone di strumenti di ricerca automatizzata analisi e correlazione evoluti – altro argomento che merita un'attività dedicata di technology tracking e per il quale è possibile offrire una soluzione centralizzata.

Utilizzate uno strumento per la rilevazione in tempo reale di attacchi informatici, intrusioni o - più semplicemente - per l'analisi sommaria del traffico di rete?

Circa metà delle sezioni utilizza F/W commerciali o open source e gli strumenti da essi forniti (che non sempre sono mirati ed efficaci); solo 3 sezioni implementano strumenti dedicati all'analisi del traffico o all'intrusion detection su rete o direttamente su host (argus, zeek/bro, ntopng. Anche questa è un'area abbastanza scoperta, e per la quale il palliativo del ricorso generalizzato a F/W commerciali potrebbe non essere possibile (essenzialmente per problemi di costo e bande da controllare). È auspicabile la formulazione di una soluzione praticabile e replicabile ovunque, e l'eventuale *creazione di un'intelligenza centrale*.

Utilizzate un firewall? Se sì, di che tipo: standard/NG, commerciale/open source, . . .;

Panorama variegato: 4 sezioni sono prive di F/W (hanno risposto NO - spero sia sottinteso che implementano ACL sul router di frontiera); 10 usano un F/W (in genere NG) commerciale, le altre F/W open source, o soluzioni miste, o ACL sui router di frontiera. C'è spazio per varare una robusta attività di studio e TT: andrebbe proposta una soluzione standard facilmente ed efficientemente implementabile in tutte le sezioni (anche valutando, eventualmente, uno schema standard di segmentazione LAN/segregazione risorse critiche per aggirare i problemi derivanti da bande troppo larghe etc.)

Vi servite di aggregatori di informazioni OSINT/indicatori di compromissione o di strumenti per la raccolta e l'analisi di informazioni OSINT sul vostro dominio? In caso affermativo siete in grado di utilizzare tempestivamente ed efficacememte gli IOC?

Solo due risposte positive, relative comunque ad attività non ancora completamente strutturate. Terreno fertilissimo per un'azione gestita centralmente: si parla ovviamente della realizzazione di un SOC che si occupi di gestire strumenti come MISP e svolga il lavora di raccolta, analisi e diffusione di informazioni security related per tutto l'ente; è allo studio anche la messa in opera di un prototipo di DNS firewall alimentato dagli IOC diffusi da CSIRT Italia. Per il momento lo CSIRT INFN inoltra alle sezione i risultati degli scan realizzati da Shadowserver, ma l'attività va rivista e strutturata meglio.

Utilizzate tool o piattaforme in grado di svolgere una o più funzioni tra configuration check, compliance assessment, audit, detection and response, vulnerability detection, threat intelligence, malware detection, log analysis, …?

Molti citano Greenbone per l'audit e risk assessment richiesto da MM, un paio Wazuh, un paio Kaspersky con una punta di nostalgia, poco meno della metà delle sezioni risponde laconicamente NO (ma suppongo che si tratti di un'interpretazione – almeno GSA dovrebbe essere un obbligo). Le attività di configuration check, compliance assessment, log analysis etc. vanno senz'altro promosse tramite l'individuazione di uno strumento comune da mettere in funzione ovunque – anche questa dovrà essere materia per il WG sulla sicurezza.

Utilizzate tool non contemplati in questo breve - e sicuramente incompleto - elenco che svolgono funzioni collegate alla sicurezza dei sistemi e delle reti? Se sì, quali?

Sostanzialmente solo risposte negative e questo denota, senza offesa, uno scarso dinamismo, pienamente – ahimè – motivato dalla mancanza di risorse da dedicare alla cybersecurity: con l'attuale organizzazione del lavoro (ognun per sé e dio – o la buona sorte, a seconda – per tutti) non riusciamo ad andare molto oltre la mera sopravvivenza, e questo è un attitudine pericolosa già sul medio periodo. La cybersecurity oramai non può più essere materia per generici brillanti: è necessario che se ne occupi personale dedicato, opportunamente formato e quindi specializzato che abbia la possibilità di aggiornarsi con costanza.

driving by the rear view mirror

- Facciamo molto, ma non tutto e in maniera disomogenea e poco organica;
- Le informazioni rilevanti rimangono confinate nelle strutture in cui gli eventi si verificano, e questa è una strategia sicuramente perdente;
- **Dispieghiamo praticamente solo strumenti reattivi** – alla luce del punto precedente è una scelta (probabilmente obbligata) particolarmente pericolosa;
- La proverbiale autonomia delle strutture in macanza di manpower adeguato rende assai problematico gestire produttivamente ed efficacemente, ciò che più importa, la sicurezza informatica dell'ente.