FormezPA

Webinar 1 -

Risposte degli esperti alle domande dei partecipanti rimaste inevase durante l'evento on line dell'11 giugno - ore 12:00-13:30 - La sicurezza informatica nella pubblica amministrazione – Webinar 1.
Esperti Giovanni AMATO e Luca LUSINI

G.G.P.: Come mai, nonostante la versione del Piano PA, Il MITD ritiene che i Server PA non siano sicuri per un'altissima percentuale? Cosa può essere migliorato per implementare le misure "minime" (ovvero adeguate ex GDPR e idonee se si considera NIS, NIS2...)?

Stime simili sono difficili da fare in modo univoco ed oggettivo per determinare lo stato di sicurezza di ogni singolo servizio erogato dalla PA.
Inoltre, i dati raccolti non sono di immediata interpretazione e non possono essere facilmente sintetizzati in due categorie (sicuri e non sicuri).
A dicembre 2020, il CERT-AGID ha scansionato 22.000 portali istituzionali censiti in IndicePA per verificarne la corretta configurazione di HTTPS e del CMS.
Pochissimi siti (<10%) avevano configurazioni completamente sicure ma l'interpretazione delle restanti configurazioni non si traduce automaticamente in "insicuri".

A.N.: Quali sono gli attacchi più frequenti in macchine Linux? Non sto parlando di server ma proprio di macchine Linux utilizzate all'interno di piccoli enti. È generalmente più sicuro per l'utilizzo dell'utente senza alcun privilegio di amministrazione?

Non abbiamo molte evidenze riguardo a malware specifici per desktop Linux. I casi di cui siamo a conoscenza riguardano botnet, RAT e miner di criptovaluta.
Niente impedirebbe di realizzare ransomware o infostealer per Linux, probabilmente il maggior fattore frenante è il poco ritorno: Linux è ancora meno diffuso di Windows nell'ambiente lavorativo, presentando quindi una minore superficie di attacco, ed è molto variegato, rendendo il furto di informazioni più laborioso.
Ad oggi ci sembra che il panorama dei malware per Linux sia finalizzato all'accesso alla macchina.
È interessante notare come la maggior parte dei danni effettuati dai malware non necessiti di privilegi utente particolari poiché malware come infostealer e ransomware possono comunque esfiltrare e/o cifrare i file dell'utente.

R.D.M.: come possiamo verificare se i nostri PC sono stati oggetto di attacchi e come individuare eventuali soluzioni?

Il personale non tecnico ha campo di azione più limitato, deve necessariamente affidarsi ad un antivirus.
Può fare attenzione anche a situazioni anomale, come la presenza di un grande numero di

messaggi di posta inviati (segno che la casella è stata compromessa).
Il personale tecnico, avendo un campo d'azione più ampio, può verificare le applicazioni avviate automaticamente (con strumenti come la suite di SysInternal, ad esempio), la legittimità dei processi in esecuzione e del traffico di rete (a livello di macchine, con strumenti tipo Wireshark o firewall). Anche in questo caso un antivirus aggiornato dovrebbe rilevare la minaccia nell'arco delle 24/48 ore.

S.L.R.: l'antivirus di Windows è più efficace di altri antivirus in commercio?

Non abbiamo mai fatto confronti tra antivirus. Windows Defender sembra una soluzione valida per quanto riguarda la sicurezza in senso stretto.
Secondo test online, è al pari degli altri antivirus (si trovano fonti discordanti, molte delle quali promuovo direttamente o indirettamente altri AV).
Gli Antivirus commerciali si distinguono per tutta una serie di caratteristiche accessorie di cui Windows Defender non dispone.

W.C.: perché One drive non è sicuro?

La domanda è stata estrapolata dal contesto. Su OneDrive, e servizi simili, la sicurezza si riduce essenzialmente alla fiducia. E' difficile che i server di Microsoft siano violati, la domanda è se le informazioni che salviamo su OneDrive siano al sicuro da Microsoft stessa.
Senza scadere in complottismi, Microsoft non è interessata ai dati o alle password dei suoi utenti, la perdita di reputazione è più onerosa di qualsiasi guadagno ottenuto dall'uso improprio dei nostri dati.
Ma Microsoft è un'azienda come tutte le altre e non sempre i processi e le persone si comportano come si vorrebbe.
Per cui, per dati veramente sensibili (leggi sicurezza nazionale o simili), è meglio evitare di dare un potenziale vantaggio strategico ad un'azienda statunitense.
Ovviamente il fatto che OneDrive sia accessibile 24/7 online da tutto il mondo espone al rischio di accessi abusivi nel caso si sia vittima di attacchi mirati od occasionali (ovvero, se vi rubano la password da OneDrive recuperano tutto).

N.D.: Google Chrome memorizza le password: è sicuro?

No, nessun browser lo è.
Le password sono salvate in chiaro, l'unico modo per renderlo sicuro è richiedervi una password per accedere alle password salvate.
Questo però è il lavoro di un password manager, i browser non si avventurano in un campo quale il salvataggio sicuro delle password (per il momento).

M.M.: Il completamento automatico dei plugin dei password manager sui browser sono effettivamente sicuri?

L'unico modo per rispondere è quello di verificare come funzionano i vari plugin tramite reverse engineering.
In teoria ci sono tutti gli estremi per renderli sicuri, in pratica (o in termini effettivi, come richiesto) non ci sono studi specifici.
Questo è un tema su cui vorremmo investigare di più, purtroppo al momento condividiamo i suoi stessi dubbi.