PERCHÉ LA PROTEZIONE MULTI-LIVELLO È IMPORTANTE

Firewall

Antivirus

Difesa proattiva dal malware

Eliminazione

Informazione degli utenti

COS'È LA PROTEZIONE MULTI-LIVELLO?

Adottare una strategia di protezione multi-livello significa sfruttare varie soluzioni di sicurezza informatica diverse che agiscano sinergicamente per ridurre la superficie di attacco di un sistema in rete.

QUALI SONO LE ULTIME SFIDE?

La maggioranza dei responsabili IT e degli addetti alla sicurezza ritiene che i rischi connessi agli endpoint sono notevolmente aumentati. Le cause:

73% uso di applicazioni cloud commerciali

63% teleloveratori e dipendenti fuori sede

68% dispositivi mobili di proprietà dei dipendenti

RESPONSABILI PIÙ FREQUENTI

Attacchi da parte di malware subiti dalle reti informatiche nell'ultimo anno (erano consentite più risposte):

- Attacchi di malware basati sul Web — 80%
- APT/attacchi mirati — 65%
- Rootkit — 65%
- Spear phishing — 55%

AUMENTO DELLA GRAVITÀ E DELL'EFFICIENZA

Il 69% degli intervistati ha dichiarato che l'aumento degli incidenti provocati da malware nell'ultimo anno è aumentato.

Nel 60% dei casi, gli aggressori possono danneggiare un'azienda nel giro di pochi minuti[1].

DOVE SONO LE FALLE NEI SISTEMI DI DIFESA?

NON SAI DI QUANTI LIVELLI

Il 97% degli attacchi osservati nel 2014 **è stato causato da appena 10 vulnerabilità informatiche**, su un totale di 7 milioni di vulnerabilità dichiarate[2].

Il **99,9%** degli attacchi che sfruttano le vulnerabilità viene effettuato dopo **più di un anno** dalla pubblicazione.

SCARSA SICUREZZA

Tempo eccessivo per rilevare le minacce, mancata adozione **di misure per contrastare le falle note,** mancata applicazione o disinformazione sulle politiche di sicurezza, mancata adozione o implementazione scorretta di tecniche crittografiche, mancanza di protezione dai **malware, configurazioni wireless deboli,** lacune a livello di sicurezza fisica, informazioni non strutturate, applicazioni legacy non più supportate, fornitori e partner commerciali non completamente protetti.

DISINFORMAZIONE O NEGLIGENZA DEGLI UTENTI

- Cadono vittime di attacchi di phishing o si fanno ingannare da altre tattiche di ingegneria sociale
- Bypassano le misure di sicurezza installando i malware direttamente nel sistema
- Comunicano le proprie credenziali durante gli attacchi di phishing
- Pubblicano informazioni sicure sui social network

DI SICUREZZA HAI BISOGNO?

Soluzioni tecnologiche

Software anti-attacco
Arcieri: includono tecnologie anti-exploit, anti-spam e anti-phishing. La tecnologia anti-exploit è in grado di fermare gli attacchi prima che possano infiltrarsi nel sistema.

Rete
Castello: se si installano tutti gli aggiornamenti e le patch previsti, il sistema operativo contribuisce alla sicurezza della rete.

Firewall
Muri del castello: includono whitelist IP, blacklist e tecnologie di sicurezza delle porte. Fungono da barriere tra il mondo esterno e la rete interna.

Anti-malware
Cavalieri: si concentrano sulle nuove minacce ed eliminano le infezioni. Possono anche rilevare software indesiderati come i PUP, tenendoli lontani dai potenziali destinatari di messaggi spam o impedendo loro di impegnare le risorse del computer.

Antivirus tradizionali
Guardie: prevengono le infezioni da virus, trojan, worm e altre minacce note.

Applicazioni che interagiscono con Internet
Cancelli: se non si aggiornano le applicazioni come Java e Flash, la rete rimane vulnerabile agli attacchi.

Soluzioni volte a incrementare la consapevolezza

- Le politiche informatiche sono documentate?
- Le politiche sono ragionevoli?
- I dipendenti rispettano davvero le politiche di sicurezza informatica?
- Sono state adottate tecnologie per verificare l'attuazione delle politiche?

L'amministratore IT consulta fonti esterne per informarsi sulle minacce e utilizza le informazioni per respingere gli attacchi. Inoltre, protegge gli utenti con politiche di sicurezza efficaci.

L'utente è **LA MISURA DI SICUREZZA PIÙ IMPORTANTE.** Un utente ben informato contribuisce a rafforzare tutti i livelli di sicurezza.

Per ulteriori informazioni sulla sicurezza a più livelli, visita il sito **www.malwarebytes.org**

Malwarebytes

Fonti:
1. 2015 State of the Endpoint Report: User- Centric Risk, studio sponsorizzato da Lumension e condotto indipendentemente dal Ponemon Institute LLC (gennaio 2015); Verizon 2015 Data Breach Investigations Report
2. Verizon 2015 Data Breach Investigations Report