SOPHOS

Checklist di tecnologie, strumenti e tecniche per una Web Protection efficace

Per essere efficace, una strategia di Web protection richiede policy che limitino la superficie di attacco, nonché strumenti e tecnologie che consentano l'implementazione di tali policy, e infine una protezione che blocchi gli attacchi ad ogni livello.

Le seguenti best practice possono essere utilizzate per sensibilizzare gli utenti sui motivi per cui le policy sono importanti per garantire la giusta sicurezza della vostra azienda.

Checklist relativa alle policy di Web protection

☐ Policy di navigazione sicura

Bloccare le categorie di siti indesiderati e inadeguati per limitare la superficie di attacco delle minacce. Le policy devono come minimo escludere le seguenti categorie:

- Siti per soli adulti, contenuti sessualmente espliciti, nudità
- Proxy anonimi
- Attività criminali, hacking
- Gioco d'azzardo
- Sostanze illecite, alcool e tabacco
- Intolleranza e odio
- Phishing, frode, spam, spyware
- Di cattivo gusto e offensivi
- Violenza e armi

Potrebbe anche essere consigliabile controllare altre categorie, nell'interesse della produttività e della larghezza di banda.

☐ Policy per l'utilizzo di password sicure

È necessario implementare policy che prevedano la creazione di password efficaci; a tale scopo, si consiglia di seguire queste linee guida:

- Utilizzare password lunghe
- Includere numeri, simboli e caratteri maiuscoli e minuscoli
- Evitare di usare voci comuni del dizionario
- Evitare di utilizzare informazioni personali come nomi o date di nascita
- Modificare sovente le password
- Evitare di annotare le password

☐ Policy di controllo delle applicazioni

Limitare il numero di browser Internet, applicazioni e plug-in utilizzati nell'azienda a un set standard, implementandone l'uso mediante apposite policy.

- Browser: adoperare un unico browser d'uso corrente che supporti l'API Google Safe Browsing, ad es: Google Chrome, Firefox o Apple Safari.
- Java: a meno che non sia richiesto da applicazioni Web indispensabili per l'azienda, disabilitare o rimuovere Java; in alternativa, è possibile limitarne l'uso agli utenti che non possono farne a meno.
- Lettori PDF: adoperare un unico lettore PDF d'uso corrente e applicare le dovute patch.
- Lettore multimediale: evitare add-on e pacchetti codec superflui. Ove possibile, attenersi alle funzionalità offerte dal sistema operativo, mantenendone aggiornate le patch.
- Plug-in, add-on e barre degli strumenti per il browser: evitare plug-in e barre degli strumenti superflui.

☐ Policy di gestione delle patch

Ove possibile, verificare che nelle seguenti applicazioni siano stati attivati gli aggiornamenti automatici, e controllare che aggiornamenti e patch vengano applicati dagli utenti non appena diventino disponibili.

- Browser Web
- Java
- Lettori PDF
- Flash Player

I seguenti tool e tecnologie sono essenziali per implementare le policy definite e fornire protezione contro i più recenti attacchi Web.

Checklist relativa agli strumenti e alle tecnologie di Web protection

☐ Filtraggio degli URL

Per implementare le policy di navigazione sicura, occorre un filtraggio degli URL efficace. Optare per una soluzione che non vi confonda con centinaia di categorie, e la cui impostazione delle eccezioni delle policy sia semplice. La soluzione ideale deve consentire agli utenti di inviare richieste di eccezioni in completa semplicità; deve inoltre permettere al personale IT di gestire tali richieste nel giro di pochi clic.

☐ Filtraggio dei siti malevoli

Per la protezione contro i siti malevoli, accertarsi di disporre di un reputation filtering. Optare per una soluzione aggiornata in tempo reale da un vendor che dispone di centri internazionali per l'analisi delle minacce in grado di individuare ininterrottamente i nuovi siti infetti.

☐ Blocco di proxy anonimi

Tenere sotto controllo gli utenti non autorizzati, utilizzando tecnologie in grado di bloccare l'abuso dei proxy anonimi per bypassare il filtraggio degli URL. Scegliere una soluzione che includa sia il blocco della categoria anonymizer che il rilevamento dinamico e in tempo reale dell'anonimia, per bloccare proxy nuovi, sconosciuti, o "fai da te".

☐ Filtraggio antispam

Verificare che la soluzione antispam utilizzata sia impostata su tecnologie aggiornate per il blocco dei messaggi di posta indesiderati, inadeguati, contenenti link di phishing o altro malware — difendendo così uno dei principali punti di accesso dei moderni attacchi Web.

☐ Scansione avanzata alla ricerca del malware proveniente dal Web

È importante che l'intero traffico Web venga sottoposto a scansioni in base alle più aggiornate tecnologie di rilevamento avanzato del Web malware. Scegliere una soluzione che sottoponga a scansione tutto il traffico (non solamente i siti più a rischio), e che lo faccia senza incidere su latenza o performance. Verificare che la soluzione utilizzata si serva delle ultimissime tecnologie disponibili, quali ad es. l'emulazione di JavaScript, per il rilevamento di minacce occultate o polimorfiche.

☐ Scansione HTTPS

Evitare l'errore di tralasciare un aspetto importante, utilizzando una soluzione di Web security che preveda la scansione del traffico cifrato. Verificare che la soluzione non influisca sulla performance e che consenta di salvaguardare la privacy degli utenti che visitano siti di banche o istituzioni finanziarie.

☐ Rilevamento del “call home”

Nell'eventualità di un'infezione, accertarsi che la soluzione utilizzata sia in grado di individuare i computer infettati all'interno della rete, identificandone le richieste verso URL di comando e controllo noti per contenere malware.

☐ Protezione degli utenti remoti

Proteggere gli utenti che navigano all'esterno del perimetro di rete aziendale con una soluzione che offra Web protection per endpoint o filtraggio in-the-cloud. La Web protection per endpoint può essere integrata all'antivirus per desktop, diminuendo la quantità di software per client da dover gestire, e offrendo nel contempo protezione Web senza bisogno di dover ricorrere al backhauling o al reindirizzamento per le scansioni in-the-cloud. Optare per una soluzione che consenta di gestire dalla stessa console sia gli utenti situati all'interno della rete che quelli remoti.

☐ Aggiornamenti in tempo reale

Verificare che il sistema offra aggiornamenti in tempo reale e senza alcun ritardo. Gli aggiornamenti dei dati delle minacce inviati ogni ora o una volta al giorno non sono più un'opzione fattibile.

☐ Controllo delle applicazioni

Implementare policy di controllo delle applicazioni che dispongano di strumenti in grado di impedire alle applicazioni indesiderate di installarsi o eseguirsi sugli endpoint. Sebbene il filtraggio del gateway di rete a livello delle applicazioni possa essere utile nell'interesse della produttività e del controllo della larghezza di banda, è importante implementare il controllo delle applicazioni sugli endpoint.

☐ Patch assessment

Semplificare l'implementazione di una strategia di applicazione delle patch, con una soluzione in grado di individuare e attribuire priorità alle patch di sicurezza più importanti per il software client Web selezionato.

☐ Antivirus e HIPS

Scegliere un prodotto antivirus per endpoint con tecnologie di host intrusion prevention system (HIPS) incorporate. Optare per una soluzione che includa regole di best practice per l'HIPS, invece di dover tirare a indovinare per scovare le più efficaci impostazioni di protezione dalle minacce.

Sophos Web Protection

Per completare questo importantissimo elenco, verificare che le suddette tecnologie possano contare sul supporto di un vendor di IT security che si dedichi a fornire il più alto livello di protezione. Scegliere un vendor che disponga di un centro internazionale per l'analisi delle minacce che scruti ininterrottamente il Web alla ricerca delle minacce più recenti, e che invii all'istante aggiornamenti sulle nuove minacce.

Optare per una soluzione che non si limiti a fornire una protezione efficace, ma che sia anche facile da installare e da gestire. Una sicurezza semplice è una sicurezza migliore.

Come avviene un attacco malware sul Web in cinque passaggi
Scarica subito

Registratevi per una prova gratuita su sophos.it
Sophos Secure Web Gateway
Sophos Enduser Web Suite

Vendite per Italia:
Tel: (+39) 02 911 808
E-mail: sales@sophos.it

NP 10/13 NSG na

SOPHOS