baramundi

White Paper

Gestione delle vulnerabilità

Identificazione automatica ed eliminazione rapida delle lacune di sicurezza

Empower your IT

SOMMARIO

1 Sfidare la sorte? No grazie!

Sempre più spesso si legge di spettacolari attacchi informatici, in cui vengono rubati o cancellati migliaia di record di dati. Questi attacchi non sono affatto il risultato di un colpo di genio di hacker di talento, ma in un numero crescente di casi sono inflitti da criminali che sono riusciti a fare centro senza attrezzature costose, né conoscenze professionali di programmazione. Utilizzano gli exploit disponibili gratuitamente online per molte migliaia di vulnerabilità che sono potenzialmente presenti su ogni client e server Windows in un'azienda. Un attacco di successo può essere sferrato attraverso ciascuna di queste falle. I firewall e gli antivirus non offrono una protezione efficace contro questo tipo di attacchi. Anche un dispositivo non configurato in modo sicuro rappresenta una minaccia e una password riutilizzata su più servizi facilita inutilmente eventuali attacchi.

Sfidare la sorte lasciando delle lacune nel sistema non è una virtù auspicabile per un amministratore IT, che è responsabile della sicurezza dei dati e del regolare funzionamento delle infrastrutture. Dati dei clienti, cifre d'affari, documenti su progetti di sviluppo – le conseguenze di un attacco informatico riuscito possono paralizzare le attività operative e rivelare informazioni aziendali riservate. Oltre alle perdite finanziarie e ai danni all'immagine dell'azienda, nel peggiore dei casi sussiste anche il rischio di indagini da parte della procura, per esempio se si sospetta una violazione della normativa sulla protezione dei dati, o se i computer aziendali colpiti sono stati collegati a una botnet e comandati da remoto per effettuare attacchi informatici. In questo caso, seguendo gli indirizzi IP gli investigatori risaliranno all'azienda.

In considerazione del numero elevato e in costante aumento di lacune nella sicurezza, è chiaro che non è assolutamente possibile per un amministratore IT mantenere una visione d'insieme e garantire in modo affidabile la massima sicurezza possibile su tutti i dispositivi terminali senza disporre di risorse automatizzate. Lo stesso vale per la configurazione dei numerosi dispositivi all'interno di un'azienda. Questo white paper descrive i pericoli che incombono e come configurare una gestione automatizzata delle vulnerabilità utilizzando un software di gestione degli endpoint, per rilevare in modo affidabile pericolose falle nel sistema e chiuderle rapidamente.

2 Dalle vulnerabilità agli attacchi informatici

2.1 Definizione: vulnerabilità, exploit & co.

Una vulnerabilità è come una finestra di casa dimenticata aperta: rappresenta un errore rilevante per la sicurezza in un sistema informatico o in un'organizzazione. Sussiste quindi la possibilità che un criminale faccia irruzione, anche se non ne esiste la certezza. Tuttavia, sarebbe imprudente lasciare la finestra aperta più a lungo del necessario.

Sarebbe pericoloso se ci fosse un exploit per quella vulnerabilità, vale a dire uno strumento appropriato in grado di sfruttare quella lacuna. Perché ora il criminale ha in mano una scala, che può usare per raggiungere la finestra aperta. Tuttavia, mentre un uomo in abiti scuri con un passamontagna e una scala di alluminio nel quartiere potrebbe attirare l'attenzione, gli exploit possono essere facilmente scaricati da Internet e nella maggior parte dei casi anonimamente. Nel tempo si è sviluppato un intero settore sommerso che sopravvive guadagnando denaro attraverso gli exploit. Il pagamento avviene semplicemente attraverso servizi come PayPal. Sono disponibili anche exploit gratuiti.

Gli exploit sono utilizzati per fare entrare nel sistema che viene attaccato il cosiddetto "payload", cioè un programma malware che spia i dati, cancella i file o rende l'endpoint parte di una botnet. In altre parole, il sacco che il ladro utilizza per nascondere e portare via il suo bottino.

Un framework come Metasploit, che è stato sviluppato in realtà come strumento per rilevare le lacune di sicurezza, consente agli utenti con un po' di esperienza anche di utilizzare gli exploit ed eseguire attacchi. Metasploit si installa con facilità su Windows o Linux, ha un'interfaccia utente grafica o controllata tramite menu ed è anche disponibile come macchina virtuale. E se questo sembra ancora troppo complicato, è possibile trovare aiuto nei forum su Internet o nelle guide rapide su YouTube. I potenziali hacker hanno quindi uno strumento facile da usare come una scala, ma molto meno appariscente.

2.2 Il ciclo di vita di una vulnerabilità

Il software è un prodotto molto complesso: secondo Microsoft, ad esempio, Windows 7 conteneva circa 40 milioni di righe di codice. Di regola, un buon software presenta meno di un errore ogni 1.000 righe di codice. Pertanto, anche con i migliori controlli di qualità, rimane aperto un numero sufficiente di falle che possono trasformarsi tutte in un problema di sicurezza informatica.

Finché la vulnerabilità giace dormiente nell'ombra, i rischi sono bassi. Tuttavia, le cose cambiano quando la finestra aperta cattura l'attenzione di qualcuno, sia esso uno sviluppatore, un esperto di sicurezza o un programmatore dilettante. Queste persone si scambiano informazioni nei forum su Internet, documentano le vulnerabilità scoperte nei database e le

segnalano allo sviluppatore del software. Grandi aziende come Microsoft o Google pagano dei premi per la scoperta di nuove lacune, in modo da poterle chiudere rapidamente.

In genere, non ci vuole molto tempo perché sia disponibile una patch appropriata che ponga rimedio alla falla. Ma questo non significa che il pericolo sia eliminato, anzi! Anche gli sviluppatori di exploit leggono i database delle vulnerabilità per informarsi sulle lacune. Analizzano le patch fornite dallo sviluppatore e cercano di capire come poter sfruttare la lacuna. Finché la patch non viene installata su tutti i dispositivi interessati dalla lacuna, possono essere sferrati attacchi efficaci sfruttando la vulnerabilità nota.

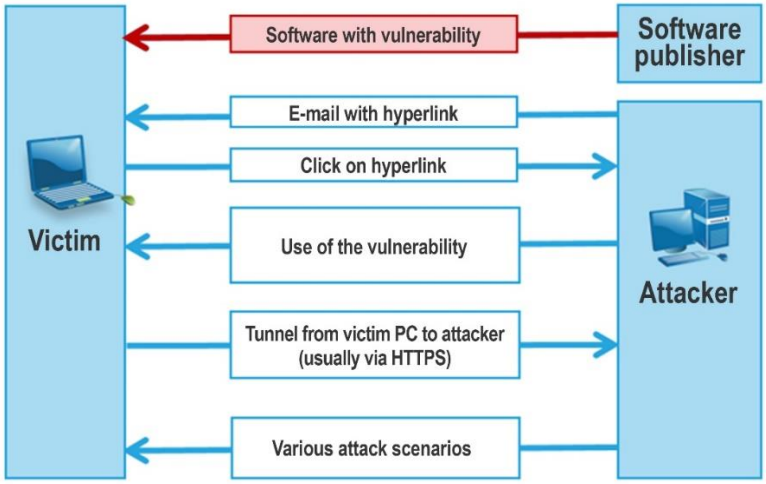
Rischio finché la lacuna non viene risolta su tutti i dispositivi

2.3 Vettori di attacco: come gestire gli attacchi al firewall

In passato, i criminali informatici di solito cercavano di bypassare il firewall per ottenere l'accesso alla rete retrostante. Tuttavia, al giorno d'oggi le misure di sicurezza sono così sofisticate ed efficaci che questo metodo generalmente fallisce.

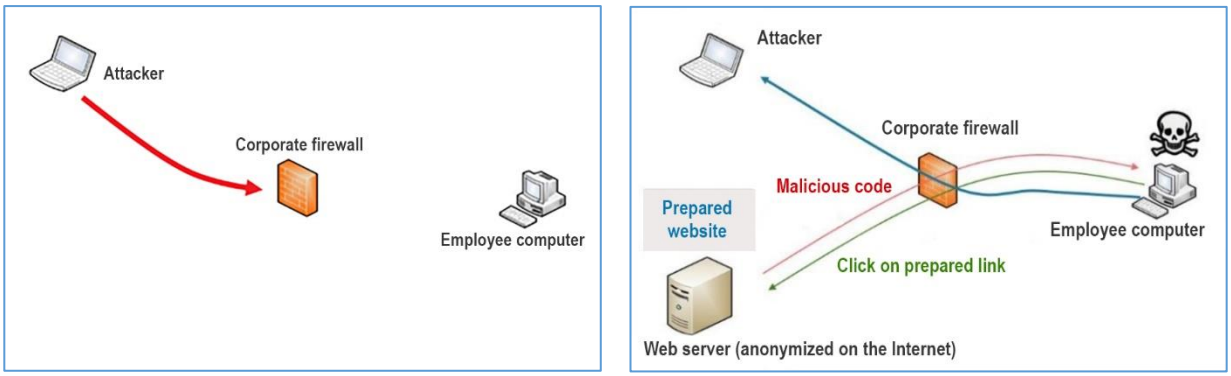
I truffatori online di oggi scelgono quindi metodi più subdoli. A volte gli attacchi vengono effettuati tramite la pubblicità su siti web in realtà innocui. Oppure gli hacker attirano le loro vittime su siti web allestiti per distribuire codice malware. Vengono utilizzati anche file manipolati che sfruttano le vulnerabilità dei programmi di visualizzazione (DOC, PDF, ecc.) passati agli utenti. Gli hacker usano informazioni dai social network e fonti simili per attirare i loro obiettivi nella trappola.

Un classico esempio: una e-mail ai dipendenti di una grande azienda con un oggetto che promette sconti sensazionali per un prodotto popolare. Senza dubbio, una certa percentuale di destinatari farà clic sul link nell'e-mail. Quello che si apre, tuttavia, è un falso webshop, che prende di mira una vulnerabilità del browser o del flash player. L'utente dopo poco, infastidito perché la pagina non si carica correttamente, chiude la finestra, ma certamente non informerà l'amministratore, dato che la navigazione privata è proibita sul posto di lavoro.



Possibile scenario di attacco attraverso una vulnerabilità del software

Se sul PC dove è stato cliccato il link era presente la falla di sicurezza, è già troppo tardi. L'attacco è riuscito. Ora c'è un malware sul computer che si mette in contatto con l'hacker. Poiché questa connessione è stata stabilita dall'interno della rete aziendale, l'attacco non può essere rilevato dal firewall.



Realizzazione della connessione con l'hacker

Un buon firewall, un software antivirus efficace e la gestione dei diritti degli utenti sono quindi ancora essenziali. Tutto ciò deve però essere integrato con ulteriori misure, quali la sensibilizzazione di tutti gli utenti e soprattutto la chiusura di tutte le lacune di sicurezza in modo coerente e il più velocemente possibile su tutti i dispositivi.

3 Identificazione e risoluzione delle vulnerabilità

3.1 La gestione manuale delle vulnerabilità non è praticabile

Di fatto è quasi impossibile per un amministratore controllare a mano tutti i PC, notebook e server nel loro ambiente per tutte le vulnerabilità conosciute. Solo negli ultimi tre anni[1], più di 80.000 nuove falle di sicurezza sono state registrate nel National Vulnerability Database[2], cioè circa 550 alla settimana. Inoltre, ci sono lacune conosciute da tempo in programmi ancora in uso, in combinazione con diverse versioni linguistiche ed eventualmente anche architetture di processore e sistemi operativi differenti.

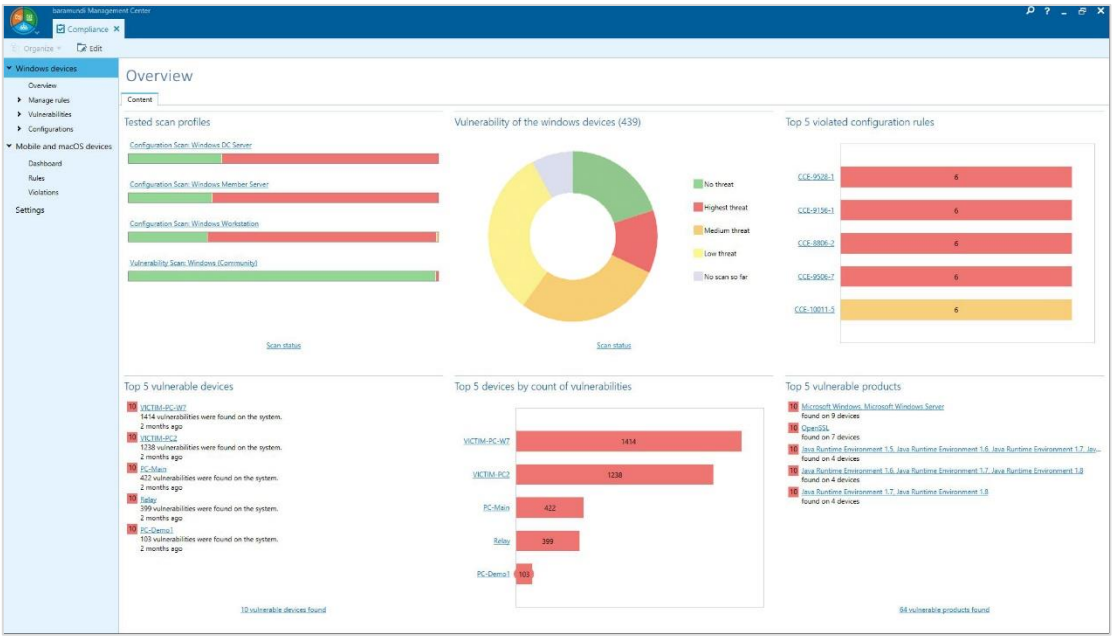
L'amministratore dovrebbe costantemente cercare nei database e nei blog le segnalazioni di vulnerabilità, valutarle, controllare i computer gestiti, confezionare gli aggiornamenti, testarli, distribuirli e verificarne l'esito. In reti più estese e in aziende con sedi distribuite e personale sul campo, questo approccio è destinato a fallire. Al contempo, il responsabile IT deve garantire la conformità dell'ambiente, essere in grado di rendicontare sullo stato delle patch, se necessario, e in casi estremi assumersi la responsabilità dei problemi.

3.2 Rilevamento automatico delle lacune di sicurezza su ogni endpoint

È possibile utilizzare strumenti di automazione, come il software di gestione degli endpoint baramundi Management Suite. Questa soluzione scansiona continuamente gli endpoint e i server nell'ambiente alla ricerca di vulnerabilità e offre la possibilità di chiudere rapidamente e centralmente le eventuali falle rilevate. Vengono monitorati sia i dispositivi collegati presso la sede centrale dell'azienda, sia i dispositivi presso siti esterni o appartenenti al personale sul campo (o in smart working).

Per svolgere questo compito, il sistema accede ai database delle vulnerabilità costantemente aggiornati di organizzazioni riconosciute. La funzione di scansione delle vulnerabilità nella baramundi Management Suite utilizza un catalogo di vulnerabilità note per rilevare le lacune di sicurezza nell'ambiente IT. Un cruscotto mostra una panoramica chiara dello stato dell'ambiente. Grazie alla visualizzazione per elenchi, è possibile eseguire il drill-down per computer, vulnerabilità o livello di minaccia, per identificare in modo mirato i dispositivi con le maggiori lacune di sicurezza, le vulnerabilità più frequentemente rilevate nell'ambiente o le falle più pericolose, al fine di risolverle il più rapidamente possibile.

[1] Da gennaio 2017 a dicembre 2019
[2] https://nvd.nist.gov



baramundi Management Suite: panoramica delle minacce all'ambiente nel cruscotto relativo alla conformità

La scansione delle vulnerabilità avviene in background, utilizzando risorse minime, e non ha impatto sul lavoro degli utenti connessi all'endpoint. Allo stesso tempo, permette di giocare in anticipo rispetto ai potenziali hacker: gli amministratori ricevono tutte le informazioni necessarie per risolvere le lacune esistenti il più presto possibile, prima che possano essere utilizzate per attacchi.

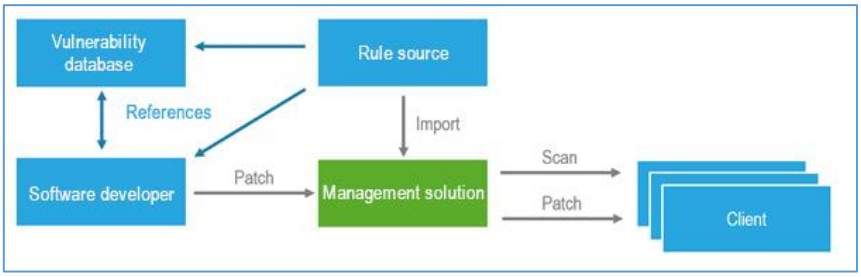
L'installazione rapida della patch riduce l'intervallo di tempo contrassegnato in rosso, durante il quale gli attacchi sono probabili

3.3 Risoluzione delle lacune di sicurezza in modo centralizzato e automatico

Per distribuire le patch e gli aggiornamenti richiesti, il software di gestione degli endpoint offre anche soluzioni automatizzate. Gli aggiornamenti per i prodotti Microsoft sono forniti tramite un modulo di gestione delle patch che provvede a inoltrare ai computer tutti gli aggiornamenti necessari in base a una serie di regole. Le installazioni vengono eseguite in background e gli eventuali riavvii richiesti sono combinati in modo da ridurre al minimo il tempo di installazione. Poiché le patch possono essere installate da più file server, il carico sulla rete rimane basso. Gli amministratori rilasciano le patch, in modalità automatica o manuale, e definiscono regole diverse per i diversi gruppi. In seguito all'introduzione delle patch cumulative da parte di Microsoft, è possibile distribuire gli aggiornamenti funzionali e di sicurezza agli endpoint e ai server in bundle.

Anche gli aggiornamenti per programmi non Microsoft vengono forniti dalle rispettive software house (ad esempio Adobe, Mozilla) sotto forma di pacchetti pronti per la distribuzione, utilizzabili anche per installazioni iniziali o disinstallazioni. Il software di gestione degli endpoint provvede altresì alla distribuzione automatica, anche su siti esterni collegati semplicemente via Internet o sui notebook del personale sul campo.

Poiché tutti i processi nella suite di gestione degli endpoint sono collegati, gli amministratori IT ricevono un feedback su ciascuno di essi e possono così sapere se l'installazione è in corso, se è stata completata correttamente o se si sono verificati degli errori. Si è così sicuri non solo che le patch di sicurezza siano state inviate, ma anche che abbiano raggiunto l'obiettivo e chiuso la falla.



Importazione di regole e patch, scansione degli endpoint per rilevare eventuali lacune e distribuzione centralizzata delle patch

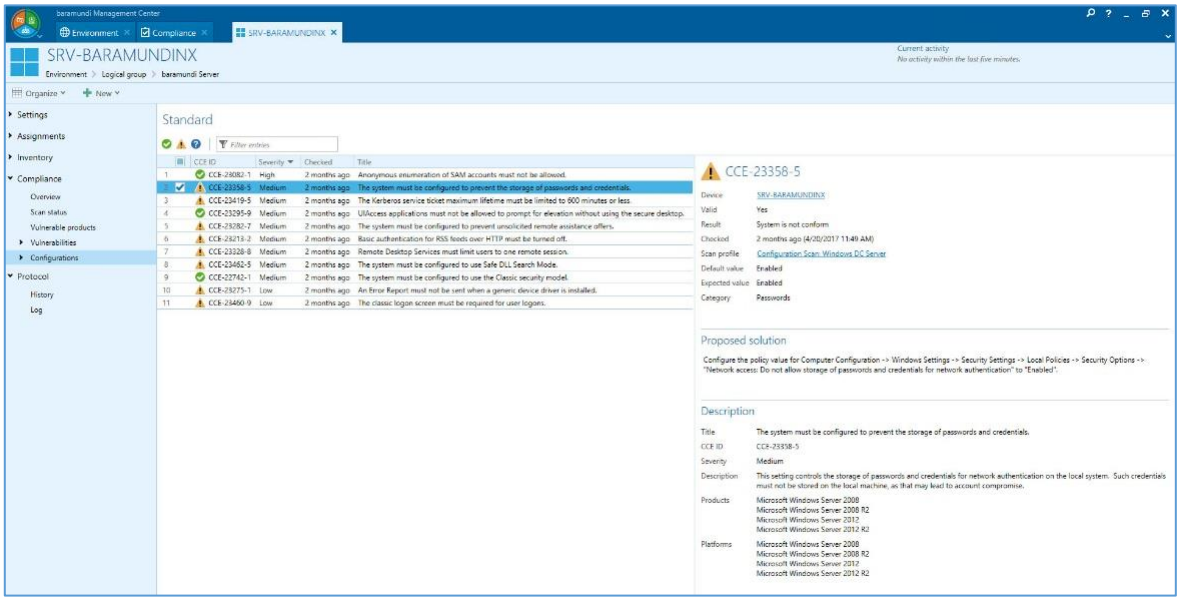
4 Gestione delle configurazioni

4.1 Applicazione di impostazioni di sicurezza

Lunghezza della password e richiesta della password dopo un periodo di inattività sono configurazioni essenziali per la sicurezza di un dispositivo. È anche importante sapere se AutoPlay è disabilitato per tutte le unità disco, quali tipi di accesso remoto sono possibili su computer remoti o se è permessa l'archiviazione delle password con crittografia reversibile.

La specifica e la distribuzione di tali impostazioni avvengono generalmente in base alle politiche di gruppo. Tuttavia, per imporre un alto livello di sicurezza, è necessario anche controllare che siano implementate su tutti gli endpoint. È infatti possibile che la configurazione sia stata modificata durante l'esecuzione di interventi di supporto o dall'utente finale stesso senza autorizzazione.

Tuttavia, proprio come per la ricerca delle vulnerabilità nelle applicazioni e nei sistemi operativi, in ambienti estesi è realisticamente impossibile per un amministratore IT tenere d'occhio la configurazione di tutti i computer senza strumenti automatizzati. Il rimedio è una soluzione per la gestione delle configurazioni, in grado di controllare il rispetto di un determinato set i regole sugli endpoint, in base ai requisiti di configurazione aziendali. Tali soluzioni – spesso in bundle con soluzioni per la gestione delle vulnerabilità – sono offerte integrate nei sistemi di gestione degli endpoint.



Risultato della verifica della configurazione su un client Windows

L'amministratore IT è così in grado di sapere quali dispositivi presentano delle violazioni. I risultati della scansione possono essere visualizzati per singolo endpoint o aggregati a livello

di gruppi e/o unità organizzative. Il sistema suggerirà anche le possibili soluzioni per correggere le violazioni in modo mirato.

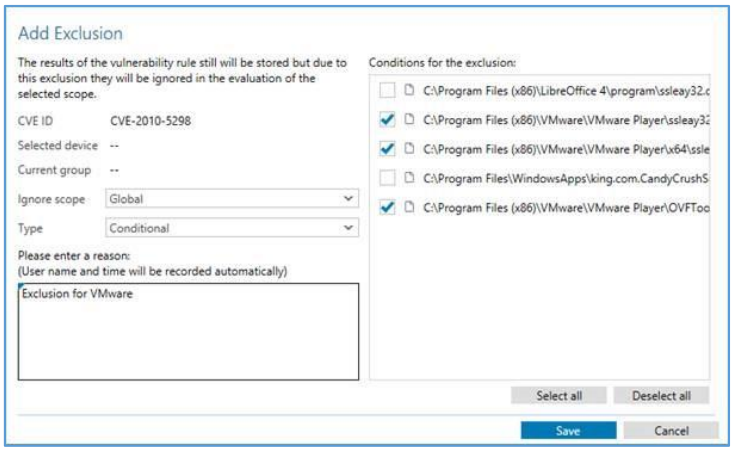
4.2 L'eccezione conferma la regola

In un ambiente IT complesso, il software utilizzato è di solito molto vario. Sui dispositivi aziendali sono installati diversi programmi software standard, software speciali personalizzati e/o vari componenti del sistema operativo. Questo software a sua volta include componenti isolati (ad esempio, librerie SSL) che potrebbero presentare delle vulnerabilità.

In qualità di utente, generalmente, non è possibile sostituire queste librerie autonomamente, senza ricevere un aggiornamento dal produttore del programma. Se l'azienda può fare a meno dei programmi colpiti, la scelta migliore è disinstallarli. In caso contrario, una valutazione di rischi e benefici può anche portare alla decisione di continuare a usare il programma e le librerie OpenSSL nella directory del programma saranno dichiarate conseguentemente come eccezioni.

Per una buona gestione delle vulnerabilità di una soluzione di gestione degli endpoint, è importante in questo caso, in primo luogo, garantire la trasparenza sull'esistenza potenziale di una lacuna di sicurezza e, in secondo luogo, offrire la possibilità di definire delle eccezioni, affinché queste vulnerabilità vengano identificate come eccezioni note e tollerate all'interno dell'azienda.

Nell'esempio qui sotto, nella baramundi Management Suite, la libreria vulnerabile è tollerata in VMware Player come eccezione, mentre lo stesso file non è accettato per LibreOffice o altri programmi.



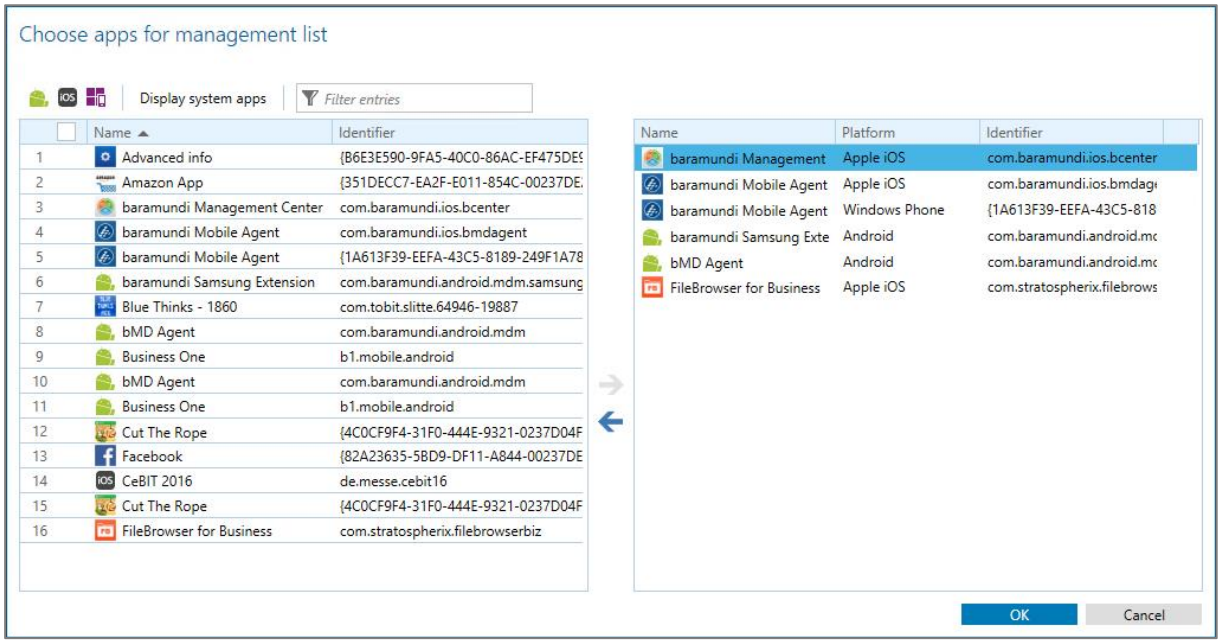
Definizione delle eccezioni per le vulnerabilità

5 Dalla gestione delle vulnerabilità alla sicurezza degli endpoint

La gestione automatizzata delle vulnerabilità e delle configurazioni è una componente efficace di una strategia di sicurezza di successo. Tuttavia, per assicurare un'elevata sicurezza degli endpoint e dei dati occorre considerare anche altri aspetti.

Ad esempio, le lacune di sicurezza devono essere rilevate anche su smartphone e tablet, che ormai si trovano in quasi tutte le reti estese, per avviare rapidamente delle contromisure. Per i dispositivi mobili, questo tipo di scansione è almeno altrettanto importante quanto per i client PC, poiché i dispositivi mobili consumer generalmente non prevedono un ruolo di amministratore tramite il quale impedire l'installazione di un software da parte dell'utente finale. Anche per questo sono disponibili strumenti automatizzati, ad esempio baramundi Mobile Devices, che è integrato nella baramundi Management Suite. Questo modulo controlla il rispetto delle regole, liberamente definibili, sui dispositivi mobili gestiti e rileva eventuali jailbreak, attacchi root o app indesiderate.

Altre soluzioni software per la gestione degli endpoint consentono di eseguire backup centralizzati e automatizzati dei dati e delle impostazioni degli utenti, di criptare supporti informatici mobili (ad es. le chiavette USB), di impedire copie illegali sui supporti di memoria removibili o di bloccare – per mezzo di blocklist e allowlist di app – l'avvio di applicazioni sconosciute e non autorizzate nella rete aziendale, supportando efficacemente l'amministratore nel garantire il miglior livello di sicurezza possibile.



Selezione delle app per blocklist e allowlist

Informazioni su baramundi software GmbH

baramundi software sviluppa Unified Endpoint Management per un' amministrazione centralizzata di PC, dispositivi mobili e server. Automatizza la distribuzione del software, semplifica la gestione delle patch e crea trasparenza nella rete. baramundi dà così un contributo significativo alla sicurezza informatica e libera tempo alle risorse.

www.baramundi.com

Volete saperne di più sulla baramundi Management Suite? Registratevi al live webinar!

Scoprite la gestione multipiattaforma per PC, server, dispositivi mobili, Mac e ambienti virtuali con la baramundi Management Suite in un webinar gratuito.

www.baramundi.com/it-training/

Saremo lieti di incontrarvi!

Contattateci!

baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany

+49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

+44 2071 93 28 77
request@baramundi.com
www.baramundi.com

+48 735 91 44 54
request@baramundi.com
www.baramundi.com

+49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

+43 1 71 72 85 45
request@baramundi.com
www.baramundi.com

+39 340 8861886
request@baramundi.com
www.baramundi.com

+41 77 280 49 79
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 401
Framingham, MA 01701, USA

+1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com