solarwinds msp

E-book

Sicurezza e documentazione:

l'importanza di uno strumento di monitoraggio e gestione da remoto (RMM) e di un sistema di automazione dei servizi professionali (PSA) a seguito dell'implementazione del GDPR

Quando si verificano i tanto temuti incidenti IT, è fondamentale disporre di due strumenti: una piattaforma di monitoraggio e gestione da remoto (RMM) consente di capire che cosa è andato storto presso il sito del cliente, mentre una piattaforma di automazione dei servizi professionali (PSA) illustra cosa è stato fatto per risolvere il problema. La combinazione di queste due soluzioni consente agli MSP di rispondere rapidamente al problema rilevato. Questo è particolarmente importante nel caso di incidenti di sicurezza in grado di influire negativamente sulle attività dell'impresa e di mettere a repentaglio la conformità alle leggi in vigore, in particolare al regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation).

La sola implementazione di piattaforme RMM e PSA all'avanguardia non consente agli MSP di offrire istantaneamente servizi di sicurezza e conformità. Soprattutto per quanto riguarda i requisiti stabiliti dal GDPR, gli MSP devono impegnarsi a utilizzare al meglio questi strumenti. Questo e-book illustra alcune idee per iniziare a prepararsi internamente alla conformità al regolamento GDPR.

L'approccio

I clienti nuovi e quelli esistenti probabilmente si rivolgeranno a voi per farsi aiutare a essere conformi al GDPR, regolamento che mira a tutelare i dati personali degli individui i cui dati sono oggetto di trattamento (vale a dire, i cittadini dell'Unione Europea i cui dati personali sono stati raccolti da un'organizzazione), come parte dell'impegno per garantire, in sostanza, la privacy dei dati. Nel panorama delle minacce di oggi, come è facile immaginare, i criminali informatici dispongono di tantissimi strumenti per irrompere nelle vostre reti e in quelle dei vostri clienti. A causa delle sanzioni salatissime previste dal GDPR, la posta in gioco è più alta che mai.

Ma, attenzione, passare a servizi SECaaS o CaaS potenzialmente redditizi non è un approccio privo di complicazioni. Le attività degli MSP devono essere sicure e conformi. In base al GDPR o a qualsiasi altra legge, sarà difficile offrire servizi di sicurezza senza occuparsi prima di tutto della sicurezza interna.

Per aiutare le imprese a mettere al sicuro i dati personali dei soggetti interessati, avete bisogno di una suite di strumenti che consenta di portare a termine il lavoro (piattaforma RMM). Cosa ancora più importante, dovrete produrre un'opportuna documentazione per provare che gli strumenti di cui vi avvalete funzionano correttamente (sistema PSA).

La vostra piattaforma RMM riceverà tante informazioni importanti dagli agenti dei clienti e il sistema PSA dovrà tenere traccia delle problematiche riscontrate e delle relative misure correttive. Che ci crediate o no, ogni singolo ticket creato dal sistema

PSA o inserito nel sistema tramite altri mezzi (e-mail, chat o portale Web) potrà rassicurare i clienti. Se il sistema RMM rileva la presenza di un antivirus obsoleto su una workstation, avere accesso all'intera procedura di risoluzione del ticket consente di produrre una documentazione trasparente della situazione e di rassicurare i clienti. La documentazione può essere ugualmente efficace per dimostrare la dovuta diligenza in materia di sicurezza, in base al GDPR. Cosa se ne ricava principalmente? A seguito dell'implementazione del GDPR, i report quotidiani, settimanali e mensili saranno più importanti che mai.

Sono tanti i servizi che gli MSP possono erogare per aiutare i clienti a prepararsi al GDPR, ma far loro comprendere la necessità della sicurezza su più livelli è fondamentale per chiudere un contratto di servizi di sicurezza. Uno dei migliori approcci durante le conversazioni per le vendite è evitare di far preoccupare eccessivamente i clienti delle tecnologie e discutere piuttosto dell'approccio all'avanguardia necessario per mettere in sicurezza i dati personali. In qualità di MSP, sapete perfettamente dove risiedono i dati dei clienti nei diversi sistemi. Provate a proporre loro un piano chiaro per la tutela dei dati e a spiegare come darete prova nei fatti di questa protezione.

Il servizio

Non è disponibile un solo prodotto in grado di preparare in modo completo alla conformità al GDPR. Tuttavia, uno dei metodi che aiutano a farlo prevede di individuare un framework di best practice. Si tratta di una distinzione fondamentale: non sono i prodotti a preparare alla conformità, ma il modo in cui essi vengono utilizzati insieme a best practice, criteri e procedure che consentono di prepararsi opportunamente al GDPR.

Fra i diversi framework, sono disponibili quelli più semplici, come lo schema Cyber Essentials del Regno Unito e i suggerimenti dell'agenzia governativa Australian Signals Directorate, quelli un po' più complessi quali il SANS/CIS 20 e COBIT, fino ad arrivare a quelli realmente complessi come il NIST 800, comprendente centinaia di pagine di istruzioni.

Non sono i prodotti a preparare alla conformità, ma il modo in cui essi vengono utilizzati insieme a best practice, criteri e procedure che consentono di prepararsi opportunamente al GDPR.

Nell'ambito dei servizi CaaS e/o SECaaS, esaminiamo le linee guida SANS/CIS 20. Questi controlli sono approvati dall'agenzia governativa del Regno Unito National Cyber Security Centre (NCSC).[1]

1. Inventario dei dispositivi autorizzati e non autorizzati
2. Inventario dei software autorizzati e non autorizzati
3. Configurazioni sicure per hardware e software
4. Valutazione e correzione continua delle vulnerabilità
5. Uso appropriato dei privilegi di amministratore
6. Gestione, monitoraggio e analisi dei registri di controllo
7. Protezione di posta elettronica e browser Web
8. Difese antimalware
9. Limitazione e controllo delle porte di rete
10. Funzionalità per il ripristino dei dati
11. Configurazioni sicure dei dispositivi di rete
12. Difesa perimetrale
13. Protezione dei dati
14. Controllo degli accessi in base al principio di sicurezza "need to know" (necessità di sapere)
15. Controllo degli accessi wireless
16. Monitoraggio e controllo degli account
17. Valutazione delle competenze in materia di sicurezza e adeguata formazione del personale
18. Sicurezza dei software applicativi
19. Risposta agli incidenti e relativa gestione
20. Penetration test ed esercitazioni del red team

Nota: le linee guida SANS/CIS 20 sono presentate in ordine di efficacia. Di fatto i primi cinque servizi "eliminano la gran parte delle vulnerabilità aziendali".[2]

Valutando rapidamente l'elenco precedente, potrete identificare le funzionalità che la vostra piattaforma RMM vi permetterà di offrire. Grazie ad alcuni controlli critici e a un monitoraggio attivo, avrete la possibilità di prevenire e di rilevare le violazioni della sicurezza dei vostri clienti. Ottimo, no? "Nel 2013, l'agenzia governativa Australian Signals Directorate ha segnalato di aver evitato almeno l'85% delle intrusioni informatiche mirate grazie all'implementazione appropriata dei primi quattro controlli."[3]

I primi cinque rappresentano i servizi di sicurezza che gli MSP devono garantire se desiderano operare nell'ambito dei servizi CaaS e/o SECaaS. È spesso possibile utilizzare la piattaforma RMM con scripting e personalizzazioni aggiuntivi per erogare questi servizi. Collegando lo strumento RMM a un sistema PSA, è possibile ricevere un avviso automatico a ogni violazione. Esamineremo i primi cinque controlli e forniremo alcuni suggerimenti utili per offrire funzionalità minime, Funzionalità avanzate e alcuni consigli per implementare controlli di compensazione, che vanno utilizzati quando, a causa di una determinata architettura o configurazione, non è possibile implementare il relativo controllo.

Rispetto a un'impresa che tenti di implementare tali controlli internamente, gli MSP sono avvantaggiati poiché dispongono già di una piattaforma RMM con funzioni di scripting e di un sistema PSA con funzionalità di creazione di ticket e generazione avvisi. Per implementare i suggerimenti qui presentati è richiesto un po' di impegno, ma essi sono applicabili all'intera base clienti. L'implementazione dei cinque controlli congiuntamente alle protezioni per e-mail e browser Web, alla protezione antimalware e al ripristino dei dati vi garantirà otto dei principali 20 controlli contenuti nelle linee guida SANS/CIS 20. Si tratta di un livello di sicurezza molto efficace.

CONTROLLO 1: INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Funzionalità minime: una soluzione RMM deve disporre di funzionalità integrate di base per rilevare tentativi di accesso non riusciti. Se non si tratta di una funzione predefinita, è necessario poter creare un controllo del registro eventi per monitorare gli accessi non riusciti nel controller del dominio. Quando un computer Windows® di un dominio o gruppo di lavoro diverso accede a un dominio Windows Active Directory® (AD), il server AD tenta di individuare il computer. Il registro di sicurezza di Windows produce quindi una serie di voci relative agli accessi non riusciti.

Prendete anche in considerazione l'ipotesi di abilitare l'accesso DHCP sul server DHCP, con cui è possibile eseguire uno script per analizzare le attività di concessione del lease per il protocollo DHCP, generalmente supportato dalle funzioni di scripting e delle attività automatizzate della piattaforma RMM.

Piccole e medie imprese dovranno assicurarsi di impostare tempi di lease lunghi per ridurre il rumore e creare uno script per ricavare l'ID evento 10 dal registro DHCP. È possibile utilizzare uno script di creazione eventi per creare una voce nel registro di

sicurezza di Windows, seguito da un controllo personalizzato del registro eventi dello strumento RMM. In questo modo, potrete conoscere il nome host, l'IP e l'indirizzo MAC di qualsiasi dispositivo che riceve un indirizzo IP sulla rete, nonché la data e l'ora dell'evento.[4]

Funzionalità avanzate: per una protezione maggiore, è possibile avvalersi di prodotti per il rilevamento delle intrusioni nella rete, ad esempio di un server basato su SaaS in abbonamento. Anche alcuni firewall all'avanguardia potrebbero includere questa funzione. In sostanza, dovrete poter registrare avvisi relativi ai dispositivi non autorizzati e tenere traccia di questi avvisi nel tempo.

Compensazione: è possibile proteggere una rete aziendale da intrusioni non desiderate implementando una rete guest per dispositivi e collaboratori esterni. Questa tecnica, nota come segmentazione della rete, consente di impedire ai dispositivi non gestiti e non autorizzati di collegarsi accidentalmente alle reti interne dei clienti. Per implementare controlli di compensazione ancora più complessi, è possibile installare un'infrastruttura con certificato 802.1X e offrire un protocollo DHCP/DNS sicuro (in cui solo i dispositivi parte del dominio Windows riceveranno un indirizzo DHCP e potranno utilizzare il server DNS) e un'autenticazione tramite indirizzo MAC (in cui solo i dispositivi presenti nella whitelist potranno comunicare tramite la rete).

CONTROLLO 2: INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

Funzionalità minime: questo controllo è strettamente collegato al precedente. Se i dipendenti dei vostri clienti possono installare software sugli endpoint, i vostri clienti sono esposti a rischi per la sicurezza. Di fatto è persino troppo facile indurre gli utenti con l'inganno a installare software dannosi per ottenere accesso a una rete. Ad esempio, in alcune truffe, gli utenti scaricano software con controllo remoto che dà ai criminali informatici l'accesso ai loro computer simulando un intervento di assistenza tecnica.

Sfortunatamente, molti MSP devono fornire assistenza per applicazioni obsolete che richiedono privilegi elevati per essere utilizzate, talvolta persino l'accesso come amministratore locale. Questo rende difficile garantire la coerenza e l'integrità del software sulle workstation dei clienti. Di nuovo, come controllo di base, potrete implementare un controllo del registro eventi nel software RMM per gli ID evento 1033, 1034 e 1035. I malware spesso utilizzano il servizio Windows Installer.

Funzionalità avanzate: Microsoft® Windows include una tecnologia per creare whitelist nota come AppLocker® che consente l'esecuzione delle applicazioni autorizzate sulle workstation e può essere gestita in modo centralizzato tramite oggetti Criteri di gruppo. Per garantire un servizio di monitoraggio, è possibile eseguire il servizio identità applicazione di Windows sul server e su tutte le workstation. AppLocker dispone del proprio registro eventi, pertanto è necessario creare uno script

per analizzare il registro eventi, utilizzare lo script di creazione eventi per creare una voce nel registro di sicurezza di Windows, quindi creare un controllo personalizzato sul registro eventi nello strumento RMM. Questo consente di rilevare qualsiasi software non autorizzato che tenta di avviarsi.

Secondo l'agenzia governativa Australian Signals Directorate, questa tecnologia è talmente essenziale che è ritenuta obbligatoria per i dipartimenti governativi e i collaboratori indipendenti.[5]

Compensazione: uno dei metodi migliori per compensare questo controllo è erogare tutti i servizi tramite un ambiente desktop virtualizzato controllato. In tal caso, solo gli amministratori potranno installare e pubblicare le applicazioni sulle workstation dell'ambiente dei clienti, cosa che rende l'ambiente resistente a eventuali manomissioni (ma non del tutto a prova di manomissione) e ne consente il ripristino alle condizioni predefinite con un semplice riavvio dell'endpoint o tramite disconnessione/nuovo accesso.

CONTROLLO 3: CONFIGURAZIONI SICURE PER HARDWARE E SOFTWARE

Funzionalità minime: non è possibile disporre di una configurazione sicura se questa può essere modificata da utenti o criminali informatici. Gli MSP focalizzati sulla sicurezza devono poter contare su configurazioni a prova di incidenti. Per cominciare, potete modificare le password predefinite su tutti i dispositivi hardware ed eventuali password archiviate offline nel sistema PSA, nonché quelle archiviate in modo sicuro, ad esempio in uno strumento di gestione delle password.

Il controllo 2, che impedisce l'installazione sugli endpoint, l'eliminazione di programmi e i tentativi non autorizzati di avviare un programma, funziona in modo ottimale se associato a criteri di configurazione fondati su solide basi. La chiave delle configurazioni software sicure e dell'utilizzo efficace di AppLocker è impiegare innanzitutto meno software. Potrete controllare la superficie di attacco per gli endpoint limitando le licenze software esclusivamente a quei programmi che occorrono per scelte aziendali realmente critiche. Se applicazioni come Java®, Adobe® Flash®, Adobe Reader® o Microsoft Silverlight® non sono necessarie, bisogna rimuoverle dall'immagine standard del cliente.

Gli strumenti RMM all'avanguardia sono in grado di ricavare l'elenco di asset software installati sugli endpoint dei clienti. Assicuratevi di consultare i clienti per identificare i software realmente necessari e quelli che possono essere eliminati, poi rimuoveteli per ridurre la complessità e aumentare la sicurezza.

Funzionalità avanzate: gli MSP di grandi dimensioni potranno provare ad aggiungere gestione delle configurazioni, packaging e pubblicazione delle applicazioni, oltre a strumenti più efficaci per la gestione delle password. Gli MSP che hanno investito tempo e risorse nelle build standard dei server e nelle immagini standard delle workstation

disporranno di un controllo delle configurazioni più efficace. Più script e automazioni è possibile integrare nella procedura, meglio è. La coerenza nell'ambiente del cliente renderà più efficaci eventuali interventi di assistenza o indagini sulla sicurezza.

Per incrementare il controllo potrete configurare in modo sicuro anche l'infrastruttura di rete, disabilitando protocolli e servizi di rete non necessari e provando a segmentare le workstation e a impedirne la comunicazione. Con l'impiego di tali pratiche potrete anche contenere gli attacchi ransomware.

Compensazione: non esiste una formula magica per configurare tutte le risorse hardware e software, ma molti fornitori e organizzazioni che operano in ambito sicurezza mettono a disposizione guide sull'hardening delle reti e best practice da impiegare in proposito. Sebbene la creazione di configurazioni hardware e software sicure necessiti di molto tempo a causa dei test e delle ricerche necessarie, è comunque fondamentale per prevenire gli attacchi sferrati dai criminali informatici.

CONTROLLO 4: VALUTAZIONE E CORREZIONE CONTINUA DELLE VULNERABILITÀ

Funzionalità minime: questo controllo si riduce nella pratica a un'opportuna gestione delle patch. Dovrete procedere con il rilascio delle patch con cadenza almeno mensile e controllare la presenza di aggiornamenti del firmware per le risorse hardware almeno ogni tre mesi. Il vostro sistema PSA è probabilmente in grado di generare automaticamente ticket a intervalli consoni per ricordarvi di verificare la presenza di eventuali aggiornamenti. Tutti i dispositivi hardware dovranno essere supportati dal fornitore e tutti i dispositivi vanno registrati, poiché, se lo fate, la maggioranza dei fornitori vi avviserà qualora per il dispositivo venga rilevata una vulnerabilità, soprattutto nel caso in cui quest'ultima possa essere sfruttata tramite esecuzione di codice da remoto. I fornitori inoltre vi informeranno non appena si rende disponibile una patch o una correzione.

Gli strumenti RMM all'avanguardia funzionano in modo ottimale se il software risiede sugli endpoint. Uno strumento RMM di qualità vi consentirà di automatizzare completamente o quasi la procedura di applicazione delle patch e di aggiornamento per sistema operativo e applicazioni di terze parti. Inoltre, esso dovrà inserire nel sistema PSA qualsiasi falla per le patch, così potrete risolvere il problema e assicurarvi che il cliente resti protetto. Dal punto di vista della conformità, assicuratevi sempre di conservare i report relativi all'applicazione delle patch.

Gli MSP dovranno includere anche i propri dispositivi insieme a quelli dei loro clienti nel piano di gestione delle vulnerabilità, così da ridurre significativamente la superficie di attacco per i clienti. Mettere in sicurezza l'ambiente degli MSP può ridurre la probabilità che parti terze si impadroniscano per scopi dannosi degli strumenti disponibili per sferrare un attacco tramite proxy.

Funzionalità avanzate: per rendere più efficace la gestione delle patch, provate a impostare una frequenza settimanale per la loro applicazione e a eseguire scansioni interne ed esterne delle vulnerabilità nella vostra sede. Tuttavia, in generale, con una configurazione che non prevede porte con accesso a Internet connesse ai vari servizi, una scansione esterna delle vulnerabilità avrà poca utilità.

Una scansione interna delle vulnerabilità e l'individuazione di dati personali senza protezione sono tuttavia fondamentali. Sapere se un endpoint presenta una vulnerabilità di sicurezza è certamente importante, ma, associando queste informazioni a una quantificazione dei rischi (in sterline, euro o altro), gli MSP potranno assegnare le giuste priorità nel ridurre il rischio globale dei clienti. Assicuratevi che le misure risolutive per i dati personali a rischio siano registrate nel sistema PSA e nei report mensili: questo potrebbe essere necessario per dimostrare e documentare il vostro impegno circa la sicurezza.

Compensazione: forse vi sorprenderà, ma configurare il sistema operativo e le applicazioni installate per l'aggiornamento automatico non è sempre l'approccio consigliato. È molto più importante fornire servizi gestiti per le patch e monitorare le percentuali di successo e di insuccesso delle patch. Una patch non testata è in grado di interrompere tutte le procedure operative di un cliente e, poiché alcune patch non possono essere annullate, le procedure di risoluzione del guasto potrebbero costare cifre ingenti ed esporvi a serie critiche (e non solo!) da parte del cliente.

CONTROLLO 5: USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

Funzionalità minime: come abbiamo detto in precedenza, il controllo dei privilegi amministrativi è un aspetto cruciale. A causa delle minacce cui espongono posta elettronica e navigazione sul Web, gli account amministratori non vanno mai utilizzati per queste attività, Questo richiede disciplina e controllo: il vostro collaboratore che si occupa del cliente dovrà essere l'unica persona con privilegi di amministratore all'interno della rete del cliente stesso. Bloccando i privilegi amministrativi locali o le autorizzazioni di amministratore di un dominio potrete ridurre le chiamate di assistenza e gli incidenti di sicurezza.

In luogo di utilizzare gli account amministratore integrati nel dominio Windows, operate dagli account utente con privilegi amministrativi, così da tenere traccia degli eventi di accesso come amministratore e associarli ai collaboratori specifici. Questo approccio inoltre evita di utilizzare una password comune per tutti i sistemi dei clienti. La password amministratore attualmente impostata per Windows va registrata offline e non deve essere utilizzata, tranne che in situazioni di emergenza. In questo modo, aggiungerete un discreto livello di protezione per voi poiché l'account amministratore rappresenta quello più comunemente utilizzato per gli attacchi di tipo brute force sui servizi desktop remoti connessi a Internet.

Per ottenere un beneficio rapido da questo controllo, è possibile creare un controllo per il registro eventi del sistema RMM per l'ID evento 4672 che informa gli MSP a ogni accesso degli utenti che dispongono di un'ampia fetta di privilegi amministrativi.

Funzionalità avanzate: per aggiungere un altro livello di protezione, dovrete avvalervi di tecnologie aggiuntive. La protezione più efficace degli account amministratori deriva dall'autenticazione a più fattori o dall'autenticazione a due fattori. Gli MSP potranno implementare tali autenticazioni utilizzando un servizio con controllo remoto tramite una piattaforma RMM dotata di protezioni mediante autenticazione a due fattori. Potrete fornire controlli efficaci imponendo l'autenticazione degli account amministratori alla console RMM tramite autenticazione a due fattori, quindi facendo accedere questi account ai server del cliente tramite un account amministratore con attributi e non condiviso.

Riflettete attentamente su come gestire i privilegi amministrativi su ampia scala, per migliaia di endpoint. Inoltre, accertatevi di prendere in considerazione la gestione dei dispositivi IoT e dei dispositivi dell'infrastruttura (router, firewall e punti di accesso wireless), così da gestire e organizzare le password al meglio. Uno strumento di gestione delle password rappresenta un investimento efficace per proteggere e gestire le password amministratore.

CONTROLLI EFFICACI DEI SISTEMI RMM E PSA

Per aiutare i vostri clienti a prepararsi opportunamente all'entrata in vigore del GDPR, avrete il vostro bel da fare: impostare gli standard di configurazione, creare, testare e implementare script e tante altre cose. Uno strumento RMM all'avanguardia vi permetterà di sfruttare funzionalità efficaci per monitorare e rispondere a eventuali incidenti che violano i controlli presentati in questo e-book. Le autorità del GDPR si aspettano una dovuta diligenza, pertanto accertatevi di implementare gli opportuni controlli e di documentare eventuali falle. Nel caso di controlli di conformità al GDPR, è probabile che dobbiate produrre la documentazione a dimostrazione dei vostri sforzi.

È opinione diffusa presso la community per la sicurezza che questi controlli funzionino in modo efficace. Erogare esclusivamente servizi di sicurezza di base spacciandoli per servizi di conformità non è abbastanza per impedire una violazione dei dati nel panorama odierno degli attacchi informatici. È il momento che gli MSP affrontino i criminali informatici implementando controlli più severi, molti dei quali sono già integrati nella piattaforma RMM in uso. Assicuratevi pertanto di sfruttare al meglio la piattaforma RMM e il sistema PSA per garantire servizi di sicurezza efficaci e registrare i vostri successi ai danni dei criminali informatici.

Note finali

1. “20 Critical Controls”, National Cyber Security Centre. https://www.ncsc.gov.uk/guidance/20-critical-controls (consultato a ottobre 2017).

2. “CIS Controls”, Center for Internet Security. https://www.cisecurity.org/controls/ (consultato a novembre 2017).

3. “Top 4 Strategies to Mitigate Cyber Intrusions: Mandatory Requirement Explained”, Australian Signals Directorate. https://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm (consultato a novembre 2017).

4. “Analyze DHCP Server Log Files”, Microsoft Windows Server. https://technet.microsoft.com/fr-fr/library/dd183591(v=ws.10).aspx (consultato a novembre 2017).

5. “Top 4 Strategies to Mitigate Cyber Intrusions: Mandatory Requirement Explained”, Australian Signals Directorate. https://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm (consultato a novembre 2017).