solarwinds msp

N4B NETWORK for BUSINESS

Distributore Autorizzato

1. Utilizzare un approccio alla **sicurezza su più livelli**

GUADAGNARE TEMPO

Che la si chiami sicurezza su più livelli o difesa in profondità, questo aspetto è fondamentale. Sebbene si tratti di un concetto antico quanto la sicurezza IT, impiegare diversi livelli di sicurezza non può considerarsi di certo una metodologia superata. Naturalmente, la scelta dei livelli più opportuni da impiegare è fondamentale. La difesa in profondità va considerata come un modo per ridurre i rischi degli attacchi implementando diversi livelli di controllo all'intero ambiente IT.

Tale approccio, tuttavia, non impedisce gli attacchi, ma consente di guadagnare tempo su eventuali malintenzionati e di proteggere l'organizzazione dagli attacchi inevitabili. Un approccio alla sicurezza su più livelli implementato in modo opportuno può far guadagnare tempo alle aziende e consente così di rispondere in modo efficace a qualsiasi attacco e a ridurre gli effetti dannosi di una potenziale violazione. In altre parole, consente di limitare l'hacking dei sistemi.

Ecco sette modi per implementarlo.

2. **Visibilità della rete** per una protezione proattiva

ANALISI PERTINENTI CHE CONSENTONO UNA PROTEZIONE PROATTIVA

La visibilità della rete consente di "scansionare e prendere in considerazione ogni elemento, individuare eventuali anomalie e applicare i criteri necessari". Il monitoring degli eventi di sicurezza di questo tipo può rivelarsi economicamente vantaggioso nel recupero di analisi pertinenti che consentano la protezione proattiva delle infrastrutture e dei dati in esse contenuti, poiché la visibilità della rete può aiutare a tenere alla larga i malintenzionati individuandone la presenza ancor prima che inizino a sferrare il loro attacco.

Sono disponibili sistemi gratuiti che offrono un certo livello di visibilità della rete; ad esempio, ThreatFinder di Alien Vault si basa sulla piattaforma Open Threat Exchange (OTX) e controlla la presenza di eventuali sistemi compromessi e di comunicazioni dannose mettendo a confronto i dati del file di registro con il database live OTX. Anche la valutazione dei dispositivi collegati alla propria rete è parte dell'approccio legato alla visibilità e TripWire offre uno strumento gratuito, SecureScam, che scansiona fino a 100 indirizzi IP presenti sulla rete interna, rilevando eventuali dispositivi smarriti o nascosti.

Maggiore è il numero dei dispositivi in rete che si collegano a Internet, più elevato è il rischio di compromissione.

3. **Protezione web** basata sui criteri

CONTROLLO, MONITORING E APPLICAZIONE DI CRITERI WEB

La protezione web rappresenta un altro livello essenziale di sicurezza poiché consente di controllare, monitorare e applicare i criteri web tramite un unico front-end. Di fatto, questo tipo di protezione viene considerato un approccio alla sicurezza basato sui criteri. È possibile far puntare più dispositivi ad un criterio centralizzato, modificabile e scalabile perché si adatti a una serie di dispositivi, invece di implementare trasversalmente impostazioni a livello di dispositivo.

Questa metodologia consente di applicare filtri web per periodo di tempo o contenuti, di eseguire controlli della larghezza di banda per impedirne la limitazione e di proteggere l'azienda da responsabilità legali.

4. **Gestione delle patch** per una maggiore sicurezza

AL PASSO CON I MALINTENZIONATI

È possibile eseguire scansioni che individuino gli schemi di attacco e applicare tutti i criteri desiderati, ma con la diffusione di nuove vulnerabilità quasi ogni giorno non è sempre facile restare al passo. Sebbene la gestione delle patch non rappresenti la panacea di tutti i mali e non impedisca la diffusione delle minacce zero-day o i rischi delle vulnerabilità dovute a patch non applicate, questo approccio costituisce comunque un ottimo supporto per non farsi cogliere di sorpresa.

È consigliabile iscriversi alle notifiche dei fornitori, tenere d'occhio i siti di notizie sulla sicurezza e applicare le patch non appena è sicuro farlo, poiché non solo serve sapere quando una patch è disponibile, ma anche assicurarsi che sia stabile. Infatti, applicare una patch instabile all'ambiente di lavoro senza testarne la stabilità potrebbe causare alla bottom-line dell'azienda danni più seri della minaccia che tale patch mira a bloccare.

5. **Crittografia** solo dove serve

ISOLAMENTO DEI DATI CRITICI

Il problema legato alla crittografia dei dati è che essa è sempre considerata troppo complessa e troppo costosa, ma in realtà, isolando solo i dati fondamentali per l'azienda e sottoponendo a crittografia solo questi, nulla di quanto appena affermato è vero.

I dati sottoposti a una solida crittografia non saranno attaccabili dalla maggior parte degli hacker, a parte gli 007 governativi, e talvolta nemmedo da loro. La procedura non è complicata; basta adottare i seguenti accorgimenti.

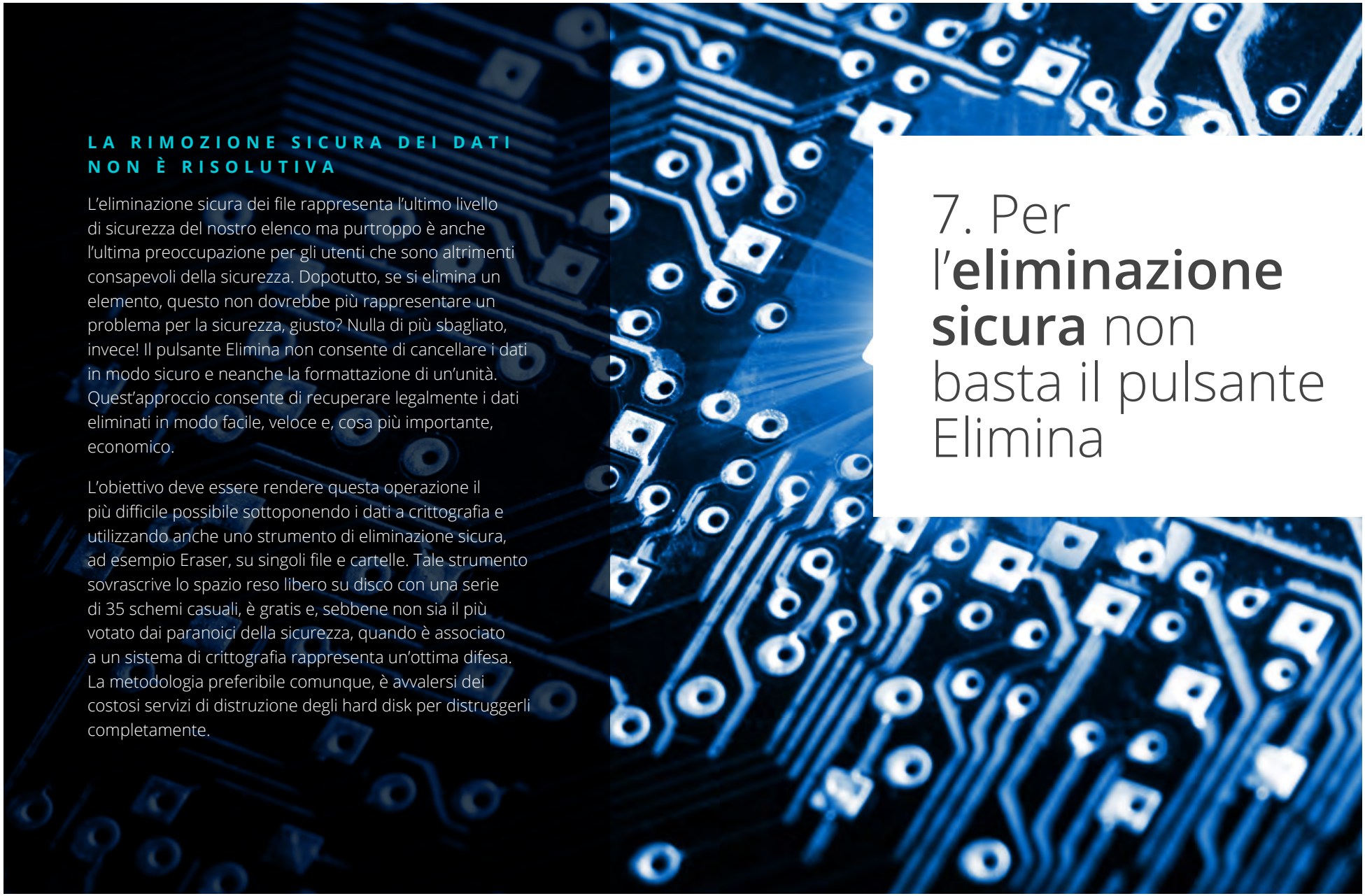
- Tablet e smartphone: la crittografia del firmware integrata nel sistema operativo rende questi dispositivi inutilizzabili dagli hacker. Non tralasciamola!
- Siti web: il protocollo HTTPS sottopone a crittografia le informazioni trasferite tra il sito e i browser dei clienti.
- Browser web: il componente aggiuntivo HTTPS Everywhere riscrive le richieste provenienti dai siti HTTP non crittografati in richieste HTTPS sicure.
- Memorie esterne USB: VeraCrypt è il programma open source di crittografia più utilizzato, poiché è facile da usare, funziona ed è gratis.

6. Autenticare, autenticare e autenticare ancora...

OPPORTUNI CRITERI DI AUTENTICAZIONE

L'autenticazione si riferisce all'utilizzo degli strumenti di gestione delle password e all'autenticazione a più fattori. La scelta di password complesse è ovvia, sfortunatamente però, qualsiasi password sufficientemente lunga, generata a caso e abbastanza complessa è anche impossibile da ricordare. Quando si tratta poi di tante password diverse, chiunque, anche dotato di una buona memoria, avrebbe difficoltà ma non gli strumenti di gestione delle password.

LastPass Enterprise è un programma di classe enterprise fra tanti: non è gratuito, ma il suo costo parte da soli 18 $ per utente e consente di gestire i criteri per le password da cloud e di generare password realmente sicure semplicemente toccando un pulsante. Ma anche questa metodologia, da sola, non è sufficiente. È necessario prendere in considerazione l'autenticazione a più fattori. È possibile aggiungere l'autenticazione a due fattori a LastPass come token fisico o codice generato da un'app per smartphone. Qualunque sia il livello di sicurezza aggiunto, l'autenticazione a due fattori rappresenta la base per qualsiasi criterio di autenticazione serio.



LA RIMOZIONE SICURA DEI DATI NON È RISOLUTIVA

L'eliminazione sicura dei file rappresenta l'ultimo livello di sicurezza del nostro elenco ma purtroppo è anche l'ultima preoccupazione per gli utenti che sono altrimenti consapevoli della sicurezza. Dopotutto, se si elimina un elemento, questo non dovrebbe più rappresentare un problema per la sicurezza, giusto? Nulla di più sbagliato, invece! Il pulsante Elimina non consente di cancellare i dati in modo sicuro e neanche la formattazione di un'unità. Quest'approccio consente di recuperare legalmente i dati eliminati in modo facile, veloce e, cosa più importante, economico.

L'obiettivo deve essere rendere questa operazione il più difficile possibile sottoponendo i dati a crittografia e utilizzando anche uno strumento di eliminazione sicura, ad esempio Eraser, su singoli file e cartelle. Tale strumento sovrascrive lo spazio reso libero su disco con una serie di 35 schemi casuali, è gratis e, sebbene non sia il più votato dai paranoici della sicurezza, quando è associato a un sistema di crittografia rappresenta un'ottima difesa. La metodologia preferibile comunque, è avvalersi dei costosi servizi di distruzione degli hard disk per distruggerli completamente.

7. Per l'**eliminazione sicura** non basta il pulsante Elimina

Informazioni su SolarWinds MSP

SolarWinds MSP offre ai provider di servizi IT tutte le tecnologie più all'avanguardia per raggiungere il successo, grazie a soluzioni che includono sicurezza su più livelli, intelligence collettiva e automazione intelligente, sia on-premise sia su cloud, e supportate da dati estremamente fruibili che consentono ai provider di servizi IT di lavorare in modo più semplice e veloce. SolarWinds MSP consente ai nostri clienti di concentrarsi su ciò che conta di più: rispettare gli SLA e offrire servizi in modo efficace ed efficiente. Per ulteriori informazioni, visitate il sito solarwindsmsp.com/it.

solarwindsmsp.com/it

solarwinds msp

N4B NETWORK for BUSINESS

Distributore Autorizzato

www.n4b.it

commerciale@n4b.it

0522-1607412

RMEB00068IT1017