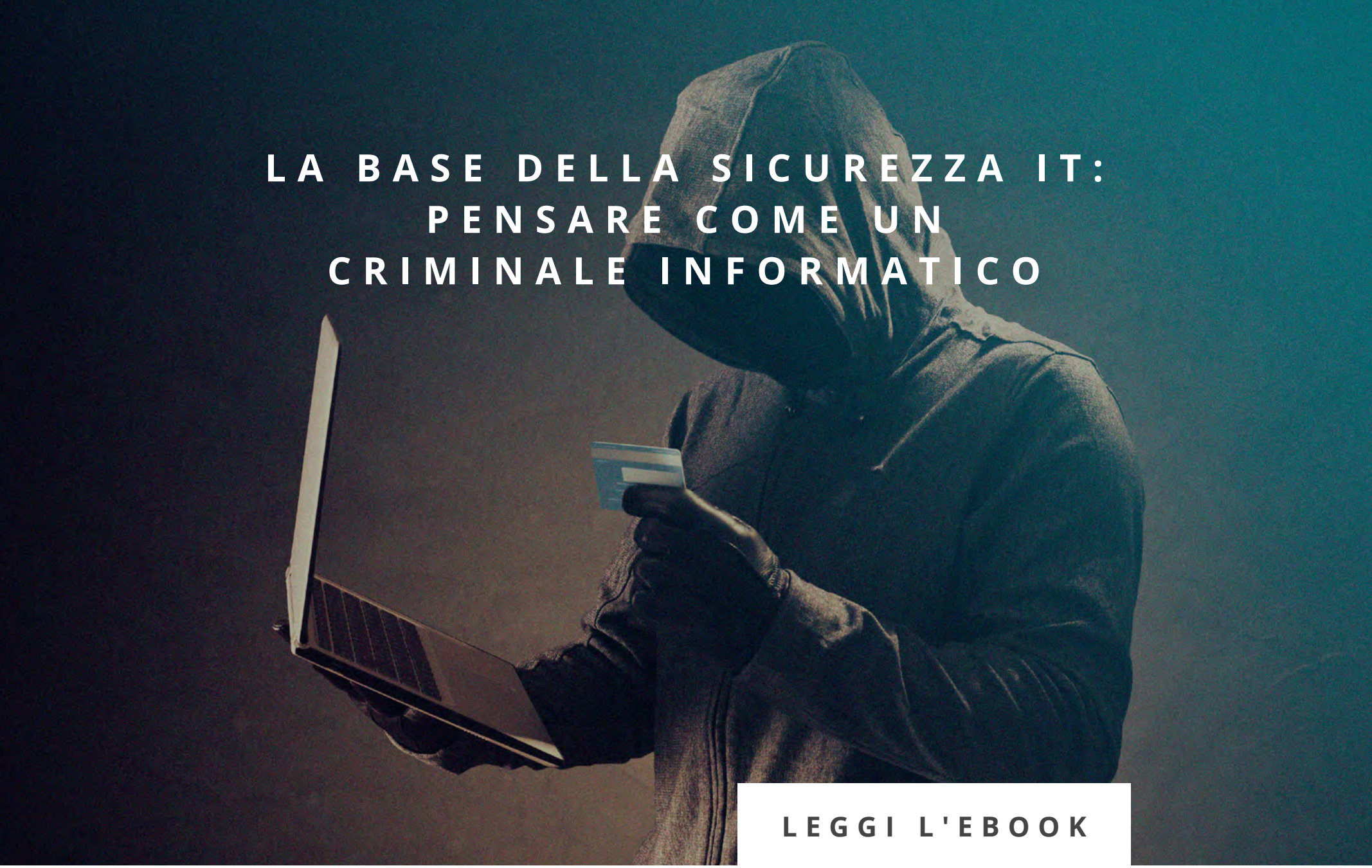

LA BASE DELLA SICUREZZA IT: PENSARE COME UN CRIMINALE INFORMATICO

LEGGI L'EBOOK

solarwinds msp

N4B NETWORK for BUSINESS

Come **pensa** un criminale informatico?

LEGGERE NELLA MENTE DI UN CRIMINALE INFORMATICO

Pensate all'approccio adottato dai detective dei romanzi: quando devono inchiodare l'autore di un delitto provano a leggergli nella mente. Nell'ambito della sicurezza IT, comprendere come evolve il panorama delle minacce è ugualmente importante. Provare a ragionare come i criminali informatici vi permetterà di proteggere in modo adeguato i vostri sistemi e dati.

Il malware rappresenta un esempio perfetto per comprendere come funzionano le violazioni di una rete. Se da una parte il malware costituisce senza dubbio il vettore di attacco numero uno per i criminali informatici, questa minaccia non costituisce l'obiettivo ultimo per tali individui. Gli autori degli attacchi utilizzano sempre più spesso il malware come modalità per andare oltre il mero accesso ai dati degli utenti: il loro obiettivo ultimo è, infatti, quello di effettuare l'escalation dei privilegi di rete per avere accesso a più sistemi e dati e controllarli. L'impiego degli strumenti per la gestione delle modifiche e dei criteri di accesso più adeguati è fondamentale in tal senso. I dati degli utenti sono importanti, ma il controllo di interi sistemi non ha prezzo.

DOVETE ARRIVARCI PRIMA CHE LO FACCIANO LORO

Applicando la stessa logica del dark web al panorama delle minacce informatiche, come credete che operino gli hacker per diffondere e dissimulare gli attacchi sferrati? Con la crittografia, naturalmente, o almeno utilizzando transazioni crittografate; in questo modo, infatti, gli hacker possono permettersi di utilizzare un minor numero di risorse per creare un codice malware sofisticato ed evitare che la minaccia venga rilevata. Comprendere che i criminali informatici utilizzano la crittografia in tal modo, vale a dire sfruttando la poca visibilità nel traffico SSL, consente di contrapporsi a tale tattica distinguendo l'utilizzo consono del traffico SSL da quello criminale. Il controllo granulare del traffico sottoposto a crittografia è fondamentale in questo senso.

Non pensate mai che il pericolo risieda esclusivamente nelle nuove minacce emergenti: gli approcci vecchio stile, infatti, ad esempio gli attacchi SQL Injection e il Cross Site Scripting sono sempre molto diffusi, mentre è cambiato l'obiettivo. In questo momento, infatti, è più probabile che gli hacker mirino ai sistemi di gestione contenuti (CMS) e soprattutto ai plug-in CMS. Anche la dissimulazione è un approccio molto comune nel caso di un attacco DDoS o DNS poisoning, sferrato per occupare le risorse di sistema, mentre l'hacker è impegnato a colpire il reale bersaglio, in genere rappresentato da un database finanziario.

Qual è l'obiettivo dei criminali informatici?

Qual è il vostro **punto debole?**

I VOSTRI PUNTI DEBOLI SONO OBIETTIVI FACILI DA RAGGIUNGERE

Adottate un approccio trasversale al panorama delle minacce e chiedetevi che cosa farebbe un criminale informatico per semplificarsi la vita. Identificare i punti deboli delle proprie reti potrebbe far comprendere molte cose agli addetti alla gestione IT. Prendiamo come esempio la semplice attività di mantenere elevati i livelli di prestazione della rete. È fondamentale, certo, ma talvolta potrebbe anche ridurre la sicurezza dell'azienda o addirittura trasformarsi in un'altra opportunità di violazione da parte di hacker senza scrupoli. In che modo? Secondo una ricerca condotta di recente da McAfee, un terzo degli amministratori IT ha ammesso di disattivare alcune funzionalità del firewall (ad esempio il controllo completo dei pacchetti in grado di rilevare attività pericolose sul traffico di rete) per migliorare le prestazioni di rete. Non semplificate le cose agli hacker solo per facilitare di poco il vostro lavoro.

6 ASPETTI DA CONSIDERARE

1. Monitorate la rete, utilizzando un servizio di tracciabilità asset anziché aggiornare manualmente grandi fogli di lavoro, per mappare e controllare i dispositivi presenti. Risparmierete tempo ed eliminerete anche gli errori legati all'inserimento manuale dei dati.
2. Formate i dipendenti, che rappresentano spesso l'anello debole della catena della sicurezza IT. Un'email di phishing, facilmente riconoscibile da un amministratore IT, potrebbe invece essere considerata assolutamente attendibile da un dipendente meno esperto in informatica. Aiutate i dipendenti a comprendere i rischi legati alla sicurezza IT.
3. Installate un antivirus all'avanguardia, che sarà essenziale nel caso in cui qualcuno selezioni un link non attendibile. Scegliete un prodotto efficace, veloce e facile da distribuire e gestire in modo centralizzato.
4. Non tralasciate l'importanza della gestione delle patch, non offerta da alcun antivirus. Una procedura e una pianificazione efficace di gestione delle patch proteggono da altre vulnerabilità, quali plug-in e componenti aggiuntivi per il web.
5. Proteggete gli utenti online che potrebbero essere facilmente ingannati da URL dannosi in grado di sottrarre informazioni aziendali e personali. Una soluzione di filtri web rappresenta un'altra linea di difesa in grado di bloccare eventuali siti web notoriamente dannosi.
6. Effettuate il monitoraggio proattivo: nessuna difesa è sufficiente a garantire la sicurezza IT se non effettuate controlli e vi limitate ad attendere che il problema si presenti in tutta la sua gravità. Installate una soluzione di monitoraggio e, soprattutto, utilizzatela.

La vostra checklist per la **sicurezza IT**

Sconfiggere i criminali informatici è possibile

ALCUNE RIFLESSIONI FINALI

Prima di tutto, dovrete, per così dire, leggere nella mente dei criminali informatici, comprendere le loro intenzioni e conoscere strumenti e metodologie utilizzati per raggiungere gli obiettivi criminali. Se riuscirete a pensare come un criminale informatico e a conoscere il suo obiettivo, avrete maggiori probabilità di difendervi.

Vale la pena ripeterlo: non semplificate le cose agli hacker solo per facilitare di poco il vostro lavoro. Le violazioni della sicurezza possono essere imbarazzanti, costose e danneggiare la reputazione di qualsiasi organizzazione, ma è possibile difendersi da tali incidenti implementando diversi livelli di sicurezza IT, grazie a tracciabilità asset, formazione dei dipendenti, software antivirus all'avanguardia, gestione delle patch, monitoraggio delle prestazioni e protezione web.

Implementare un sistema di sicurezza IT efficace rappresenta un'attività complessa, ulteriormente ostacolata dalla minaccia dei comportamenti noti e sconosciuti dei criminali informatici. Iniziate adottando i sei semplici approcci illustrati nel presente e-book e affrontate in modo proattivo le potenziali minacce restando sempre aggiornati: leggete le ultime novità in tema di sicurezza IT, informatevi sull'evoluzione del panorama di minacce e adottate le misure più opportune a seconda delle circostanze.

Informazioni su SolarWinds MSP

commerciale@n4b.it
0522 1607018
Via Sant'Ambrogio 4/2
42122 Reggio Emilia (RE)

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.

solarwindsmsp.com

RMEB00076IT0917