Ethical Hacking Penetration Test

SCHEDA SERVIZIO

Crescono esponenzialmente gli attacchi ai sistemi IT

Nonostante i crescenti investimenti in sicurezza informatica, il numero e la gravità degli attacchi continuano ad aumentare: 2/3 degli incidenti non vengano nemmeno rilevati dalle vittime.
(Fonte: academia.edu)

Sono le "infrastrutture critiche" a registrare la crescita percentuale maggiore degli attacchi gravi negli ultimi sei mesi, passando da 2 attacchi nella seconda metà del 2014 a 20 da gennaio a giugno 2015.
(Fonte: Rapporto Clusit 2015)

Una multinazionale italiana del settore fashion, ha dichiarato di aver subito un attacco informatico "sofisticato", che ha causato la sottrazione dei bozzetti di una delle collezioni di abbigliamento e di replicare gli abiti.
(Fonte: Rapporto Clusit 2015)

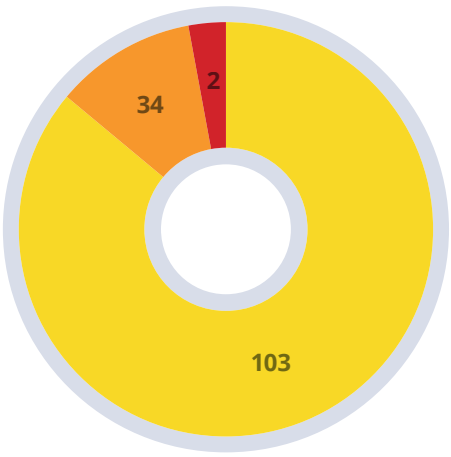
Il 40% delle organizzazioni, nel 2014, è stato sotto attacco hacker.
(Fonte: OAI, Osservatorio Attacchi Informatici in Italia, rapporto 2014)

Gli incidenti relativi alla sicurezza IT sono aumentati a livello mondiale del 66%.
(Fonte: CyberEdge Group)

In Italia i danni complessivi derivanti da attacchi informatici ammontano a circa 9 miliardi di euro, inclusi i costi di ripristino
(Fonte: McAfee)

Il danno economico mondiale causato dagli attacchi hacker si aggira tra i 375 e 575 miliardi di dollari l'anno, più o meno quanto il Pil del Belgio.
(Fonte UNICRI)

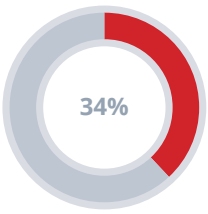
Numero medio di vulnerabilità per server



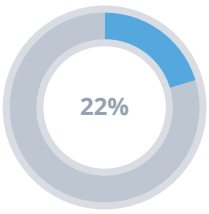
- Rischio basso
- Rischio medio
- Rischio elevato

(Fonte: edgescan)

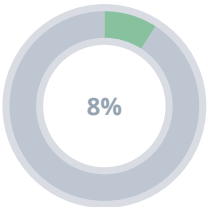
Percentuale di server con vulnerabilità



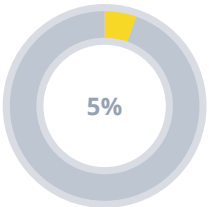
Patch di sicurezza



Configurazioni errate



Servizi esposti



Sistemi non supportati

(Fonte: edgescan)

Le minacce informatiche sono in continua crescita: è necessario avere un approccio consapevole, verificando la sicurezza dei propri sistemi IT, adottando comportamenti, azioni e misure per tutelare gli asset fondamentali delle aziende rappresentati da dati, informazioni e clienti. Mettere on-line il proprio business così come utilizzare connessioni LAN e wireless è divenuta una pratica consolidata, farlo in modo sicuro è un'azione responsabile.

Nel 2015 DFIR, il più attendibile report investigativo mondiale, ha rilevato ottanta mila incidenti di sicurezza e più di duemila violazioni di dati costate mediamente 2,8 milioni di euro.
Alcuni hacker causano danni per puro divertimento, altri mirano a impossessarsi di informazioni aziendali e personali per rivenderle a concorrenti o manipolarle, in modo da accedere a fonti finanziarie e sottrarre denaro. Basta cliccare su un link contenuto in una semplice e-mail o utilizzare un software obsoleto per diventare vittime di un attacco criminale, del quale è difficile accorgersi visti i tempi rapidissimi di esecuzione.
Le aziende sono responsabili dei dati dei loro clienti. Quando un hacker entra in possesso di account e password, le conseguenze ricadono sull'azienda stessa, in termini di scarsa affidabilità e conseguente danno di immagine; senza contare quelli economici e i problemi legati al non essersi adeguati alle normative.

La normativa del Garante della Privacy

> *"Il titolare del trattamento è **obbligato ad adottare misure di sicurezza idonee** a ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o trattamento dei dati personali non consentito o non conforme alle finalità della raccolta (articolo 31 del Codice).*
> *In particolare, il titolare deve adottare le misure minime di sicurezza (articolo 33 del Codice e Allegato B al Codice) volte ad assicurare un livello minimo di protezione dei dati personali.*
> ***L'omessa applicazione delle misure** minime di sicurezza è punita con la sanzione amministrativa del **pagamento** di una somma **da diecimila euro a centoventimila euro** (articolo 162, comma 2 bis del Codice) e con la **sanzione penale dell'arresto fino a 2 anni** (articolo 169 del Codice)."*
> Fonte: Garante della Privacy

Misure di sicurezza

Recuperare la propria credibilità professionale richiede onerosi investimenti di tempo e denaro: da una parte l'azienda è chiamata a risarcire i clienti attaccati, dall'altra a risolvere l'incidente in condizione di emergenza.
Come difendersi? Come garantire sicurezza e protezione ai propri clienti e partner?

La miglior difesa è l'attacco

Il servizio Ethical Hacking di AD Consulting

Per difendersi da attacchi di malintenzionati, il modo più efficace è mettere alla prova il livello di sicurezza della struttura aziendale, tentando di violarla come farebbe un hacker.
I consulenti di sicurezza AD Consulting, professionisti esperti e certificati, eseguono simulazioni di attacchi reali alle aree aziendali più strategiche e sensibili. Gli attacchi simulano le azioni che un malintenzionato realizzerebbe contro un'azienda: quando viene individuata una vulnerabilità, questa viene sfruttata per accedere a sistemi e risorse o per la ricerca di altre falle.
Le vulnerabilità vengono segnalate dai consulenti di sicurezza secondo un indice di pericolosità, definito in funzione del business aziendale.
Solo a questo punto si può correre ai ripari ed eliminare i rischi di compromissione, in base ai dettagli tecnici e alle indicazioni di alto livello fornite dal consulente di sicurezza su ogni specifica vulnerabilità individuata.

Come prepararsi all'impatto e correre ai ripari

Penetration Test

I consulenti di sicurezza propongono vari test, utili a rilevare vulnerabilità e a evitare incidenti:

- **Web Application Penetration Test**
- **External Penetration Test**
- **Internal Penetration Test**
- **Wireless Penetration Test**

Web Application Penetration Test

Il WAPT consente di individuare le vulnerabilità presenti su un'applicazione web, come un sito e-commerce o un portale.
Il test prevede l'individuazione e lo sfruttamento delle vulnerabilità per mostrarne i reali rischi, ad esempio il furto dei dati dell'azienda e dei clienti e attacchi verso gli utenti del sito.

Network Penetration Test

Il test consente di individuare le vulnerabilità presenti sulla rete aziendale, ad esempio sul servizio di posta elettronica, sugli strumenti amministrativi e di gestione IT, sui tool di accesso remoto e sulle VPN.
Il controllo può essere effettuato dall'esterno o dall'interno della rete, avendo in questo modo una capacità di visione e di analisi estremamente ampia.
Gli attacchi che riproduce sono quelli che può portare un malintenzionato da qualsiasi dispositivo connesso a Internet, un dipendente o un fornitore il cui account sia stato violato, un dipendente infedele, un dispositivo connesso alla rete aziendale che sia stato compromesso, ad esempio uno smartphone o il pc di un utente.

Wireless Penetration Test

Il test consente di individuare vulnerabilità sulle reti wireless, come in caso di una copertura troppo ampia, l'utilizzo di password non adeguate o la presenza di reti guest e di produzione non correttamente segmentate. Attraverso questa verifica, i consulenti di sicurezza AD Consulting evidenziano e sfruttano le vulnerabilità per accedere a porzioni di rete e negare il servizio Wi-Fi, impedendo la connessione.

Report

Al termine dell'attività, viene redatto e fornito un report dettagliato, che elenca tutte le vulnerabilità rilevate e i passaggi che sono stati eseguiti per riprodurre l'attacco. Ad ogni vulnerabilità viene assegnato un indice di rischio, definito in base alla criticità del business aziendale. Il consulente fornisce quindi indicazioni precise sulle contromisure da adottare per mettere in sicurezza la struttura aziendale.
Il report presenta inoltre un Executive Summary, utile a fornire al management una visione di alto livello di quanto rilevato.

Certificazioni

OSCP - Offensive Security Certified Professional

OSWP - Offensive Security Wireless Professional

AD Consulting

AD Consulting è focalizzata sulla progettazione di soluzioni e servizi per sviluppare e utilizzare al meglio le infrastrutture ICT. Forte di competenze tecniche e consulenziali, l'azienda sostiene i propri clienti con un'offerta completa e integrata. Aziende private e pubblica amministrazione si affidano AD Consulting per le loro esigenze di IT Governance, Sicurezza, Engineering e Software.

L'approccio all'Information Security che AD Consulting adotta è di tipo metodologico e conforme agli standard vigenti. I nostri specialisti seguono e aiutano i clienti a governare per intero i processi di sicurezza integrando con efficacia le diverse tecnologie.
L'assessment relativo alla sicurezza individua eventuali criticità e struttura un percorso efficace di adeguamento delle procedure aziendali per aumentare la sicurezza globale dell'infrastruttura, riducendo i rischi per il business e diminuendo l'area di esposizione alle minacce.