

Test di intrusione di Axians

Con il nostro servizio potete validare costantemente la postura di sicurezza della vostra azienda e presentarla alla direzione aziendale in modo conciso.



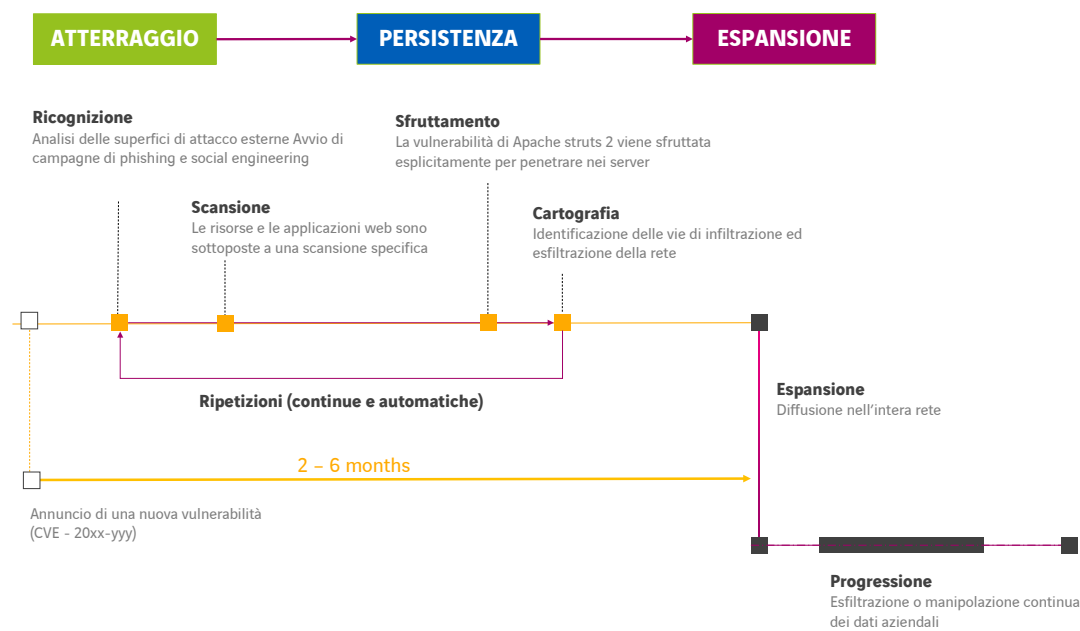
ISO 27001

LE VOSTRE MISURE DI CYBERSICUREZZA SONO ATTUATE A RAGION VEDUTA?

Test di intrusione di Axians

L'elaborazione dei dati in ambienti cloud agili, le applicazioni web e aziendali con accesso mobile, i terminali e le postazioni di lavoro esposte creano una superficie di attacco senza precedenti per la criminalità informatica organizzata. Gli esperti di sicurezza e le autorità di regolamentazione raccomandano a maggior ragione di implementare strategie di difesa informatica che validino e verifichino le vulnerabilità dell'infrastruttura aziendale anche dal punto di vista degli avversari. Tradizionalmente i test di intrusione vengono eseguiti manualmente da esperti di cybersicurezza. I relativi risultati vengono analizzati e presentati sotto forma di rapporti dedicati. Una simile validazione della sicurezza così statica e una tantum non soddisfa più i requisiti odierni di un'infrastruttura IT in continua evoluzione. Allo stesso modo, non è più opportuno che i test di intrusione si concentrino su dati e ambienti critici, poiché la pratica degli attacchi ransomware „ben riusciti“ dimostra che sono stati preparati nella rete senza che nessuno se ne rendesse conto per settimane e mesi e trovano la loro origine in sistemi presumibilmente non critici.

Anatomia di un attacco informatico: atterraggio - perseveranza - espansione



Gli hacker preparano attacchi informatici e ransomware a lungo termine e osservano le infrastrutture aziendali per lunghi periodi di tempo per colpire al momento giusto. Osservate anche voi la vostra infrastruttura aziendale costantemente e a lungo termine e colpite al momento giusto!

Axians offre il servizio giusto per affrontare ogni criticità

A partire dalla piattaforma dei test di intrusione automatizzati di Pentera, Axians offre la possibilità di sottoporre il vostro ambiente di prodotto a una validazione continua della sicurezza - controllata, sicura e trasparente!

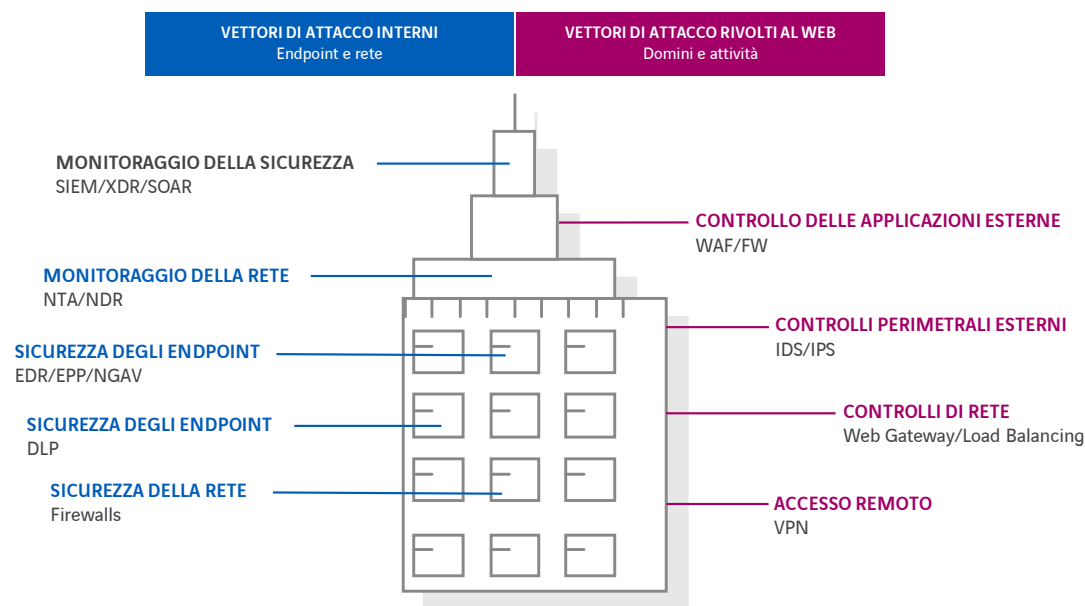
Axians vi mostra quali sarebbero le reali conseguenze di un attacco informatico sui vostri dati e processi aziendali critici e vi aiuta a rispondere alle seguenti domande:

- ▶ **La mia azienda può essere compromessa da un attacco ransomware?** In caso affermativo, quali conseguenze avrebbe nell'immediato e come si può colmare questa lacuna di sicurezza?
- ▶ **I programmi e le soluzioni di cybersicurezza sono attuati correttamente** per garantire un'adeguata protezione dagli attacchi?
- ▶ **Vengono rispettati i processi di escalation in caso di attacco** e i fornitori di servizi esterni e interni adempiono ai contratti di servizio?

La nostra offerta di servizi

Controlliamo la vostra infrastruttura aziendale in modo olistico e continuo per individuare eventuali lacune nella sicurezza, senza interrompere la produttività dei vostri dipendenti o impegnare ingenti risorse nel reparto IT. Riceverete rapporti dettagliati e raccomandazioni di intervento, aggiornati quotidianamente e personalizzati in base agli effettivi punti deboli vulnerabili.

Servizio di validazione della sicurezza e test di intrusione end-to-end



Validazione completa della sicurezza di tutti i vettori di attacco e delle risorse digitali

I seguenti scenari di test di intrusione sono menzionati a titolo di esempio e saranno adattati in modo individuale e modulare alle vostre esigenze nell'ambito di un rapporto di consulenza.

- ▶ Controllo di sicurezza dei **sistemi di elaborazione dati operativi** (per esempio, server, client, soluzioni di sicurezza per gli endpoint)
- ▶ Verifica della sicurezza delle **soluzioni di cybersicurezza e dei sistemi di controllo** (per esempio, firewall, accesso remoto e VPN, ambienti cloud, servizi di SOC)
- ▶ Controllo di sicurezza di **servizi e applicazioni rivolti al web** (per esempio shop online, e-banking, servizi web e applicazioni online)

Le nostre offerte PenTest in sintesi

Test di intrusione interna o esterna, PenTest di applicazioni web, controllo delle vulnerabilità una tantum o continuo: per garantire che nessuna falla nella sicurezza rimanga scoperta, la nostra offerta comprende vari tipi di test di intrusione. Queste soluzioni possono anche essere combinate tra loro, a seconda del progetto e delle esigenze. Non esitate a richiedere una consulenza personalizzata.

Test di intrusione delle applicazioni web

- ▶ Indagine tecnica sulle applicazioni web (compresa l'infrastruttura del server su cui viene eseguita l'applicazione) dal punto di vista di un hacker esperto.
- ▶ I test di intrusione si basano sulla Guida dell'OWASP sui test di sicurezza delle applicazioni web (in inglese WSTG).
- ▶ I PenTester eseguono 'exploit etici' ed estendono i loro test in modo strutturato con attacchi specifici derivanti dalla loro pluriennale esperienza.

Test di intrusione per API web

- ▶ Verifica tecnica dell'API web (compresa l'infrastruttura del server che ospita l'API) da parte di un hacker esperto.
- ▶ I test di intrusione si basano sulla Guida dell'OWASP sui test di sicurezza delle applicazioni web e sulla direttiva dell'OWASP sui 10 principali rischi di sicurezza dell'API.
- ▶ I PenTester eseguono 'exploit etici' ed estendono i loro test in modo strutturato con attacchi specifici derivanti dalla loro pluriennale esperienza.

Test di intrusione delle app mobili

- ▶ Verifica tecnica delle applicazioni mobili rispetto al MASVS (standard di verifica della sicurezza delle applicazioni mobili dell'OWASP), che stabilisce i requisiti di sicurezza per le applicazioni mobili.

Test di intrusione interno

- ▶ Validazione continua della sicurezza completamente allineata al framework MITRE ATT&CK. La nostra offerta è disponibile come servizio continuo o come pacchetto iniziale una tantum. Siamo a vostra disposizione per una consulenza personalizzata e sarà un piacere sottoporvi un nostro preventivo.
- ▶ Emulazione di ransomware e valutazione della sicurezza dell'AD.

Test di intrusione della superficie di attacco esterna e identificazione degli asset critici

- ▶ Validazione continua della sicurezza dei controlli perimetrali difensivi, come il controllo delle applicazioni esterne (WAF), l'accesso remoto (SSL/VPN) e i controlli perimetrali (FW), compreso il "monitoraggio delle credenziali trapelate" (powered by Pentera).

Siete interessati?

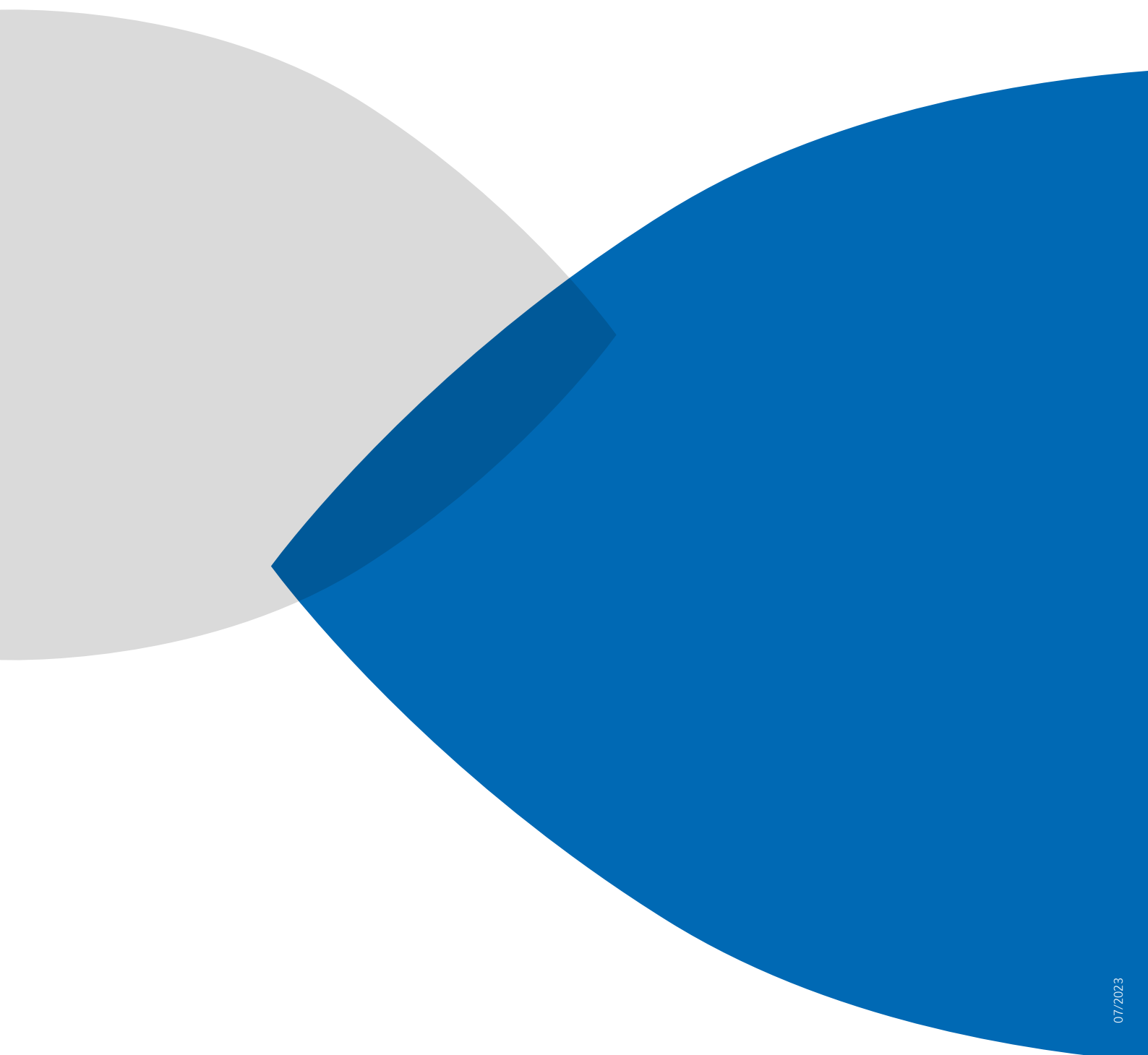
Nell'ambito di un incontro vi forniremo un servizio di consulenza non vincolante e adatteremo le offerte di PenTest affinché rispondano esattamente alle esigenze della vostra azienda.



LA VOSTRA REFERENTE

Renata Rekić (Presales Consultant)

E-Mail: renata.rekic@axians.com



07/2023

axians

Axians IT Services AG · Arlesheim · Lausanne · Zürich

Zurigo Tel.: +41 61 716 70 70

E-Mail: info-ch.security@axians.com · www.axians.ch