REPORT

Le 100 principali aziende in Italia

Report sulle minacce per la sicurezza informatica

SecurityScorecard

Introduzione

Il presente report analizza la sicurezza informatica delle prime 100 aziende in Italia per capitalizzazione azionaria.

Per guidare un'automobile è necessario un tachimetro, mentre per fare il medico serve uno stetoscopio.
Nel campo della sicurezza informatica, purtroppo, si brancola nel buio.

Il detto dice: "ciò che non si può misurare non si può migliorare". Diversi anni dopo l'attacco ransomware che ha fatto chiudere l'oleodotto Colonial Pipeline, nel mondo manca ancora un framework standard per misurare i rischi informatici. SecurityScorecard fornisce una valutazione immediata e precisa dei rischi per la sicurezza informatica, grazie a un sistema di rating dalla A alla F che si basa su dati di intelligence ricavati attraverso il monitoraggio continuo delle minacce.

Così come una posizione creditizia sfavorevole è associata a una maggiore probabilità di default, un rating di cybersecurity negativo è associato a una maggiore probabilità di subire una violazione dei dati o altri eventi informatici sfavorevoli. Le aziende con un rating pari a F potrebbero subire una violazione dei dati con una probabilità 13,8 volte maggiore rispetto alle attività con un rating di A. I rating di SecurityScorecard mettono a disposizione un linguaggio universale per la sicurezza informatica.

Per le aziende con rating A è

13 VOLTE MENO PROBABILE

subire un attacco informatico rispetto a quelle con rating F

Risultati principali

Alle prime 100 aziende in Italia è stato assegnato un punteggio in base a diversi fattori di sicurezza informatica, tra cui: sicurezza della rete, infezioni malware, sicurezza degli endpoint, frequenza di applicazione delle patch, sicurezza delle applicazioni e condizioni del DNS. Attraverso l'analisi completa della superficie di attacco e delle violazioni dichiarate, i data scientist di SecurityScorecard hanno rilevato quanto segue:

1. **Il 95% delle aziende ha subito una violazione nel proprio ecosistema di terze parti**

2. **Il 97% delle aziende ha subito una violazione nel proprio ecosistema di quarte parti**

3. **La totalità delle aziende italiane con rating di A non ha registrato alcuna violazione nell'ultimo anno** (il che dimostra l'importanza di ottenere il rating A)

4. **Al 41% delle aziende è stato assegnato il rating C o inferiore**

5. **Solo il 3% ha registrato una violazione diretta nell'ultimo anno**

6. **Il settore assicurativo vanta il più solido approccio alla sicurezza in Italia: nessuna azienda del settore ha meritato, infatti, un rating pari o inferiore a C**

   I settori ingegneristico ed edile guadagnano il secondo posto, con solo il 10% delle aziende con rating C o inferiore.

7. **I settori IT e delle telecomunicazioni meritano i rating complessivi più bassi, con l'80% delle aziende con rating pari a C o inferiore**

Risultati

Rating complessivi

1. **Il 23%** ottiene una A
2. **Il 36%** ottiene una B
3. **Il 23%** ottiene una C
4. **Il 15%** ottiene una D
5. **Il 3%** ottiene una F

Rating	Probabilità di violazione
A	1x
B	2,9x
C	5,4x
D	9,2x
F	13,8x

Il costo medio globale di una violazione dei dati è pari a 4,5 milioni di dollari.

IBM Security, Cost of Data Breach Report 2023

Panoramica del settore

Rischi informatici della supply chain

Le vulnerabilità della supply chain rappresentano un agevole punto di ingresso per i criminali informatici che intendono accedere a sistemi e reti aziendali. Le aziende di qualsiasi dimensione sono sicure quanto il loro anello più debole, il che significa che persino le attività che investono ingenti somme di denaro si trovano comunque ad affrontare i rischi dovuti alle vulnerabilità di terze e di quarte parti.

Secondo una precedente ricerca condotta da SecurityScorecard, il 98% delle aziende ha rapporti con una parte terza che ha subito almeno una violazione. Nel report, i settori con il rating di sicurezza più basso sono caratterizzati da complesse superfici di attacco a causa dell'elevato numero di fornitori di terze, quarte ed ennesime parti.

> "L'ecosistema di fornitori rappresenta un bersaglio molto ambito per i gruppi di ransomware. Le vittime di violazioni di terze parti spesso non sono consapevoli di un incidente finché non ricevono una richiesta di riscatto, il che lascia agli hacker tutto il tempo per penetrare in centinaia di aziende senza essere rilevati".
>
> **– Ryan Sherstobitoff, Vicepresidente senior di Threat Research and Intelligence**

Comunicazioni

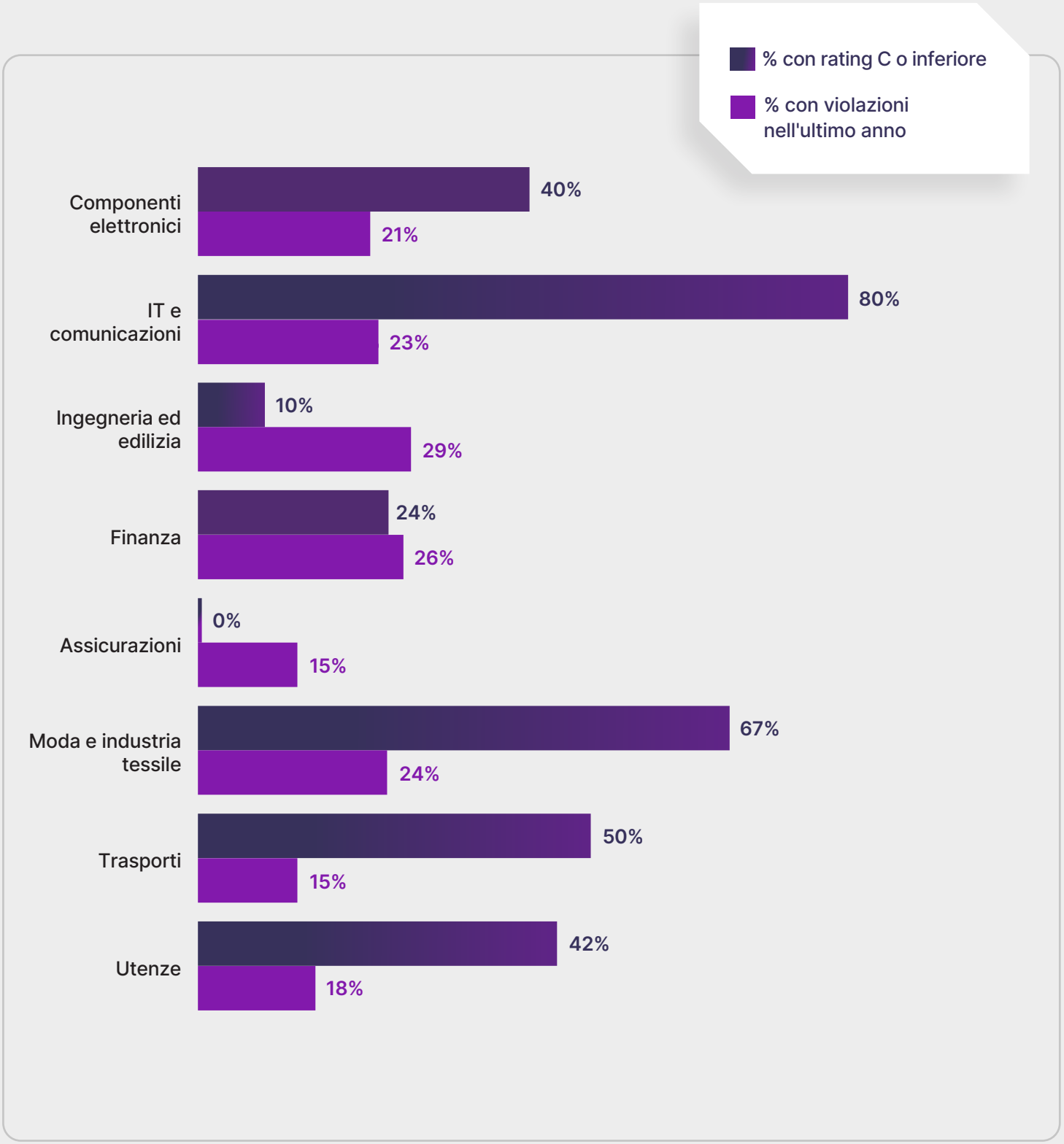
Le aziende dei settori IT e delle telecomunicazioni ottengono i rating di sicurezza complessivi più bassi: l'80% riceve un rating pari a C o inferiore. Questo non sorprende, considerato che entrambi i settori hanno superfici di attacco complesse, che comprendono ampie reti di fornitori, partner e provider di servizi di terze parti.

I provider cloud, gli operatori di servizi Internet e di telecomunicazioni consentono una connettività globale, offrono accesso a una serie di informazioni in tempo reale e trasformano le procedure operative aziendali. Hanno inoltre dato il via a innumerevoli innovazioni, favorendo il progresso della società; tuttavia rappresentano i bersagli principali degli attacchi a livello nazionale e di altri criminali.

Assicurazioni

Come menzionato in precedenza, quello assicurativo è il settore più solido in Italia, con zero aziende cui è stato assegnato il rating C o inferiore, mentre il settore edile e ingegneristico guadagna il secondo posto, con solo il 10% delle aziende con un rating pari a C o inferiore.

Rating per settore



Rating a confronto per paese

L'interconnessione del mondo digitale fa sì che la sicurezza informatica oltrepassi i confini delle varie nazioni e le reti presenti nelle varie aziende, il che rappresenta una complessità a livello globale. Per questo motivo, la condivisione delle informazioni e la collaborazione tra governi, settori e aziende sono fondamentali per garantire la resilienza informatica collettiva.

Sebbene la presente analisi si riferisca principalmente alle aziende sul territorio italiano, essa ha anche preso in esame i dati relativi alle principali aziende nelle vicine Germania, Francia e Regno Unito. I dati mostrano che le aziende britanniche sono dotate di una sicurezza informatica complessivamente più solida (con il 24% con rating C o inferiore) rispetto alle controparti francesi, italiane e tedesche (con rispettivamente il 40%, il 41% e il 34% con rating C o inferiore).

Inoltre, la Francia registra il più alto tasso di violazioni per i fornitori di terze e quarte parti (98% e 100%, rispettivamente) rispetto a Regno Unito, Germania e Italia.

SecurityScorecard di recente ha pubblicato il Global Third-Party Cybersecurity Breach Report, in un momento in cui le violazioni delle supply chain dominano le prime pagine dei giornali. Uno degli elementi chiave del report riguarda il fatto che il 75% delle violazioni di terze parti aveva come obiettivo la supply chain per software e tecnologia. Questo aspetto è risultato evidente negli ultimi anni, con diverse violazioni dei dati di alto profilo attribuite a SolarWinds, Log4j e MOVEit.

Concentrazione dei rischi informatici: una preoccupazione crescente

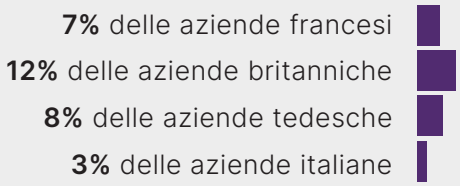
Secondo il Global Cyber Resilience Scorecard, dieci gruppi di malintenzionati sono responsabili del 44% degli incidenti informatici globali, con il gruppo C10p che risulta il fautore più prolifico delle violazioni di terze parti.

La prevalenza di pochi gruppi responsabili di danni su una scala tanto ampia indica preoccupazioni ancora più grandi circa la concentrazione dei rischi nell'economia globale. Il report di SecurityScorecard, "Redefining Resilience: Concentrated Cyber Risk in a Global Economy", con il contributo di McKinsey and Company che ha fornito dati e informazioni, si occupa proprio di questo problema. L'aspetto più significativo che emerge da tale studio è che solo 15 aziende controllano il 62% dei prodotti e dei servizi tecnologici in tutto il mondo.

Proprio per la loro enorme influenza, queste aziende potrebbero potenzialmente arrecare danni in qualità di terzi ai clienti, a causa della quota di mercato estremamente significativa e delle vaste superfici di attacco. Tali vulnerabilità rappresentano la causa principale dei tanti recenti attacchi di alto profilo alle supply chain, che hanno paralizzato settori fondamentali. Ne è un esempio l'attacco informatico ai danni di Change Healthcare, uno dei principali elaboratori di richieste di risarcimento mediche negli Stati Uniti. L'attacco del febbraio 2024 ha costretto l'azienda a scollegare oltre 100 sistemi e ha messo a rischio di chiusura molti fornitori.

Benchmarking

Aziende che hanno subito violazioni nell'ultimo anno



Aziende con rating A che non hanno registrato alcuna violazione nell'ultimo anno

Aziende che hanno subito una violazione attraverso l'ecosistema di terze parti

"La gestione dei rischi delle parti terze è fondamentale per qualsiasi adeguata strategia di cybersecurity e se diventasse una priorità, le aziende ne beneficerebbero grandemente. I settori e le aziende in Germania (e in tutta Europa) devono darsi da fare adesso se vogliono prepararsi all'implementazione del DORA (Digital Operational Resilience Act), previsto per gennaio 2025, oltre che della direttiva NIS2. L'aumento delle violazioni di dati in Europa dimostra che le aziende tedesche devono integrare la gestione dei rischi di terze parti non solo nella propria strategia di sicurezza, ma anche nella procedura di selezione dei fornitori.

SecurityScorecard viene in aiuto in tal senso mettendo a disposizione un sistema di rating atto a valutare i potenziali fornitori e a monitorare quelli esistenti così che si assumano le proprie responsabilità".

- Stefano Volpi, Direttore vendite, Italia

I rischi per la supply chain vanno oltre le parti terze

Le parti terze generalmente vengono sottoposte alla maggior parte dei controlli della supply chain, ma anche i fornitori di quarte parti pongono, a loro volta, rischi significativi.

Questo report dimostra che il 95% delle aziende ha subito una violazione tramite l'ecosistema di terze parti. Secondo un'ulteriore analisi, il 97% delle principali aziende italiane ha subito una violazione tramite l'ecosistema di quarte parti. Tali minacce sottolineano l'importanza di comprendere e valutare l'approccio alla sicurezza di tutte le parti coinvolte nell'ecosistema digitale di un'azienda.

Un fornitore che subisce la compromissione tramite una parte terza o quarta può danneggiare un ampio numero di clienti, o di clienti dei clienti, in un colpo solo. L'exploit MOVEit è stato scoperto nella primavera del 2023 e tutt'ora le aziende si stanno occupando delle conseguenze negative della violazione che, secondo le stime, costerà almeno 65 miliardi di dollari.

Ulteriori dati sulla capitalizzazione azionaria

Nonostante possa sembrare incoerente, la nostra analisi dimostra che le prime 50 aziende per capitalizzazione azionaria (da 2 a 6 miliardi di dollari) hanno un rating di sicurezza più basso rispetto alle restanti 50 aziende con una capitalizzazione azionaria inferiore (da 500 a 2 miliardi di dollari). In media, il 30% delle aziende con una capitalizzazione azionaria inferiore hanno un rating C o inferiore, mentre una media del 52% delle aziende a maggior valore ha un rating C o inferiore. Ciò dimostra che qualsiasi azienda, a prescindere da dimensioni, settore, valore o ricavi, può diventare l'obiettivo dei criminali informatici in assenza di difese informatiche adeguate.

Complessivamente, comunque, sembra ci sia una correlazione tra l'esposizione ai rischi informatici di un paese e il relativo PIL. Secondo il summenzionato Cyber Resilience Scorecard, la prosperità economica di una nazione è strettamente collegata alla sua capacità di farsi strada nel complesso panorama di minacce informatiche. Medio Oriente, America del Nord, area del Pacifico, oltre che Europa settentrionale, occidentale e centrale, registrano i rating di sicurezza più alti di tutto il mondo. In altre parole, le aree geografiche con un PIL pro capite più alto tendono a mostrare un'igiene informatica più adeguata e rischi informatici inferiori. Considerando che l'Italia (e altri paesi europei) è tra le nazioni con valori più alti di PIL pro capite, dovrebbe presumibilmente disporre delle risorse necessarie per investire in infrastrutture resilienti e sicure e per attuare e gestire iniziative di sicurezza atte a contrastare le minacce informatiche la cui natura è in costante evoluzione. È inoltre più probabile che i paesi più ricchi come l'Italia impieghino software con licenze, aggiornati regolarmente con le opportune patch di sicurezza.

Importanza della messa in sicurezza delle infrastrutture business-critical

Quasi il 40% delle aziende di questo report appartiene a settori critici: utenze, telecomunicazioni, trasporti e finanza. Perché la società funzioni al meglio, i cittadini devono fidarsi del fatto che i servizi e le istituzioni siano sicuri. Le aziende appartenenti a questi settori potrebbero trarre vantaggio dai suggerimenti seguenti. Per ulteriori linee guida e best practice, consultare il report di SecurityScorecard per il 2023, "Addressing the Trust Deficit in Critical Infrastructure".

Suggerimenti

Per molte aziende italiane, la priorità principale deve essere migliorare l'approccio alla sicurezza informatica. Sebbene la maggior parte abbia un rating di cybersecurity relativamente alto, quasi tutte le aziende hanno subito almeno una violazione attraverso terze e quarte parti. Per ridurre il rischio e migliorare l'approccio globale alla cybersecurity, SecurityScorecard consiglia di adottare le misure descritte di seguito.

Concentrarsi sulla sicurezza delle applicazioni e delle reti: per tutte le aziende migliorare la sicurezza di applicazioni e reti deve essere in cima alle priorità. Questo è fondamentale per tutelarsi da un'ampia varietà di minacce informatiche.

Aziende ad alto rischio: il 41% delle aziende con rating di cybersecurity pari a C o inferiore necessitano di un intervento più immediato. Oltre a migliorare la sicurezza di applicazioni e reti, queste aziende ad alto rischio devono focalizzarsi in particolare sugli aspetti seguenti.

CONDIZIONI DEL DNS: è necessario verificare le condizioni e l'integrità del Domain Name System (DNS). Configurazioni non adeguate di tale componente critico possono esporre a vulnerabilità.

SICUREZZA DEGLI ENDPOINT: è necessario rafforzare la sicurezza di tutti gli endpoint, inclusi laptop, desktop, dispositivi mobili e dispositivi personali. Identificare e risolvere eventuali vulnerabilità per tali endpoint è fondamentale.

FREQUENZA DI APPLICAZIONE DELLE PATCH: è necessario stabilire una frequenza coerente e tempestiva per l'applicazione delle patch per sistemi, software e hardware. Gli aggiornamenti frequenti contribuiscono a ridurre le vulnerabilità note.

Ogni azienda non solo deve essere consapevole del proprio rating, ma anche dei fattori che lo influenzano. Ogni azienda può ottenere un report dettagliato del proprio rating gratuitamente.

Conclusioni

Affidabilità e trasparenza sono aspetti cruciali della cybersecurity. Ciononostante, molte aziende non riescono a valutare adeguatamente la loro posizione rispetto alla sicurezza informatica. Il nostro studio sulle principali aziende italiane sottolinea il valore critico di questi principi.

La valutazione della cybersecurity è un processo continuo. I rating di sicurezza offrono ai responsabili della cybersecurity i dati necessari per prendere decisioni informate, rafforzare la posizione di sicurezza e favorire la collaborazione in caso di aumento dei rischi.

Nel panorama di minacce in continua evoluzione, i punteggi di sicurezza e le soluzioni di monitoraggio delle parti terze rappresentano un impegno proattivo volto a garantire la sicurezza informatica. Crediamo fermamente che ogni azienda inclusa nel presente studio abbia le potenzialità per raggiungere una posizione di resilienza e contribuire a un mondo più sicuro e collaborativo.

Metodologia

Un panorama di minacce estremamente dinamico richiede la valutazione del rischio in tempo reale. I rischi informatici vanno valutati partendo da dati aggiornati al minuto. SecurityScorecard raccoglie quantità significative di dati non invasivi circa le prestazioni di cybersecurity delle aziende di tutto il mondo. Utilizzando questi dati, possiamo valutare le difese informatiche di queste aziende. Generiamo un rating globale, dalla A alla F, in base a dieci fattori predittivi di possibili violazioni della sicurezza.

Periodo di analisi

Il presente report analizza la posizione rispetto alla cybersecurity delle prime 100 aziende in Italia per capitalizzazione azionaria, dal 13 marzo 2023 al 13 marzo 2024.

Appendice

Cosa sono i rating di sicurezza?

SecurityScorecard offre alle aziende una panoramica completa della posizione di sicurezza delle aziende, che include i rischi associati a terze e quarte parti.

I rating di sicurezza si basano totalmente sui fatti; ogni aspetto viene valutato attraverso osservazioni trasparenti, partendo dall'analisi dell'intero spazio IPv4. In correlazione ai dati di incidenza, i fattori analizzati da SecurityScorecard offrono informazioni dettagliate che aiutano le aziende a gestire gli aspetti che richiedono maggiore attenzione per ridurre l'esposizione ai rischi. I dieci fattori presi in esame sono illustrati di seguito.

Sicurezza della rete: verificare la presenza di porte aperte (come SMB e RDP), di certificati SSL poco sicuri o non correttamente configurati, di vulnerabilità dei database e IoT

Condizioni del DNS: verificare la presenza di configurazioni non adeguate, come resolver aperti, e verifica delle configurazioni raccomandate per i protocolli DNSSEC, SPF, DKIM e DMARC.

Frequenza di applicazione delle patch: misurare la frequenza degli aggiornamenti per servizi, software e hardware di un'azienda.

Sicurezza degli endpoint: misurare le versioni e l'utilizzabilità come exploit di laptop, desktop, dispositivi mobili e dispositivi personali che accedono alle reti aziendali.

I segnali della reputazione IP vengono raccolti dal sistema sinkhole di SecurityScorecard che acquisisce milioni di segnali malware da infrastrutture di comando e controllo (C2) requisite da tutto il mondo. Gli indirizzi IP con infezioni identificati vengono mappati alle aziende interessate.

Il punteggio Hacker Chatter viene ricavato da indirizzi sottotraccia o del dark web in cui vengono citate le aziende e gli indirizzi IP oggetto di attacco.

Perdita di dati: contiene le credenziali compromesse ed esposte a seguito di violazioni o perdite di dati, dump di keylogger, pastebin, database e altri repository di informazioni.

Social Engineering: prevede la misurazione dell'utilizzo degli account aziendali in social network, account finanziari e newsletter di marketing.

I punteggi Cubit vengono calcolati mediante l'algoritmo proprietario delle minacce di SecurityScorecard che valuta una serie di problemi critici per quanto riguarda sicurezza e configurazioni, ad esempio pannelli di controllo amministrativi esposti.

Per saperne di più e creare un account gratuito, visitare SecurityScorecard.com

INFORMAZIONI SU SECURITYSCORECARD

Fondata da investitori di classe mondiale come Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital e altri, SecurityScorecard rappresenta il leader globale per i punteggi, le misure e la resilienza informatica con oltre 12 milioni di aziende valutate su base continua.

Fondata nel 2013 dagli esperti di sicurezza e rischi Aleksandr Yampolskiy e Sam Kassoumeh, la tecnologia brevettata di assegnazione punteggi di SecurityScorecard viene scelta da oltre 25.000 aziende per la gestione dei rischi d'impresa, la gestione dei rischi di terze parti, la segnalazione al CdA, la due diligence, la sottoscrizione di polizze assicurative informatiche e i controlli normativi.

SecurityScorecard contribuisce a rendere il mondo più sicuro trasformando il modo in cui le aziende comprendono, migliorano e comunica i rischi di sicurezza informatica ai CdA, ai dipendenti e ai fornitori. SecurityScorecard è conforme al Federal Risk and Authorization Management Program (FedRAMP), il che conferma i robusti standard di sicurezza implementati in azienda atti a proteggere i dati dei clienti ed è stata definita uno strumento e un servizio informatico gratuito dallo U.S. Cybersecurity & Infrastructure Security Agency (CISA). Ogni azienda ha il diritto universale di ottenere un rating SecurityScorecard istantaneo, affidabile e trasparente. Per ulteriori informazioni, visitare la pagina securityscorecard.com o il nostro profilo LinkedIn.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io

©2024 SecurityScorecard Inc. Tutti i diritti riservati.