DINTEC
CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

CAMERE DI COMMERCIO D'ITALIA

Nome Cliente
Data di elaborazione: 24/05/2022

INDICE DI ESPOSIZIONE CYBER

PARTNER TECNOLOGICO

YOROI®
TINEXTA GROUP

COSA FA VEDERE?

- Le prime e più veloci informazioni accessibili sui potenziali rischi cyber che l'azienda sta correndo (senza alcuna scansione attiva all'interno dell'azienda)

QUALI INFORMAZIONI FORNISCE?

- La dimensione del perimetro digitale esposto in rete (tanto più grande maggiore sarà il rischio)
- Le vulnerabilità già note in relazione a quel perimetro (note vuol dire che sono già "sfruttate" dai cyber criminali)
- I furti di dati dell'azienda già avvenuti e presenti nel dark web (in particolare se le e-mail aziendali e le relative password sono state compromesse)

A COSA SERVE?

- A capire se occorre approfondire subito alcuni aspetti specifici
- A definire meglio eventuali ulteriori azioni necessarie per ridurre il rischio cyber

DA DOVE PROVENGONO I DATI DELL'INDICE DI ESPOSIZIONE CYBER?

L'indice di esposizione cyber viene estratto a partire da un complesso e innovativo sistema di monitoraggio e analisi delle informazioni che circolano su Internet: la **Threat Intelligence**

Threat Intelligence è l'insieme organizzato di conoscenza sugli attacchi digitali; essa racchiude informazioni relative alle scansioni continue, effettuate su Internet, integrate dalla costante correlazione di dati e informazioni eseguite a partire da "fonti" informative tecnologiche. Tra le "fonti" della threat Intelligence possiamo annoverare, senza pretesa di esaustività

- Le **Sorgenti OSINT (Open Source Intelligence)**: fonti di libero accesso che possiedono la conoscenza di base sull'andamento di minacce note. Sono fondamentali per comprendere come le minacce evolvono nel tempo e quali indicatori possono aiutarci a ricondurre i singoli data leak ad attacchi noti.
- Le **Private Source**: fonti "proprietarie", racchiudono informazioni relative a minacce individuate e bloccate da opportuni sistemi di scansione e attraverso una rete di sensori opportunamente dislocati e in ascolto sulla rete Internet
- Le **Hidden Sources (deep e dark web)**: fonti "nascoste" ad accesso ristretto, frutto di un costante lavoro di studio e ricerca, racchiudono preziose informazioni relative alle possibili future minacce, come per esempio il monitoraggio delle nuove versioni di malware e le nuove tecniche di attacco.
- Le **Classified Sources**: fonti "classificate", sono informazioni altamente confidenziali, tipicamente ottenute tramite collaborazioni con enti di Intelligence

PER CAPIRE LE INFORMAZIONI OTTENUTE OCCORRONO PARTICOLARI COMPETENZE?

No, qualunque tecnico a supporto dell'azienda con una minima conoscenza di informatica è in grado di leggere il report e di effettuare le azioni immediate di remediation necessarie laddove il report evidenziasse alcune criticità

A CHI POTENZIALMENTE INTERESSANO QUESTE INFORMAZIONI?

- Ai cyber criminali per verificare se un'azienda appare essere più o meno debole
- All'azienda per adottare eventuali procedure e contromisure tecnologiche per ridurre i rischi
- A un cliente dell'azienda per verificare se i suoi fornitori appaiono essere aziende che si preoccupano del rischio cyber
- Ad una banca che sta per affidare un'azienda
- Ad un'assicurazione che sta valutando una polizza per rischi cyber
- Ad un potenziale acquirente di quell'azienda

QUALI RISCHI CORRE OGGI UN'AZIENDA?

- **Ransomware** (paralisi dell'attività, perdita definitiva di dati fondamentali, necessità di pagare uno o più riscatti)
- **Furto di dati sensibili** (danni reputazionali, rischi di sanzioni per il mancato rispetto della GDPR)
- **Furto di identità** (danni economico-finanziari, problemi legali, segnalazioni in centrale rischi, impossibilità di accedere al credito bancario)
- **Perdita di competitività** (perdita di clienti strategici, perdita di know-how aziendale, necessità di dover aumentare i prezzi di vendita per recuperare danni subiti, diminuzione della capacità di attrarre talenti)

MA LA VERA DOMANDA CHE DOVRESTE PORVI OGGI E'……

IL RISCHIO CYBER PUO' ANCORA ESSERE IGNORATO?

Segue un esempio di Report come quello che otterrete per la vostra azienda

Grazie

Marco Castaldo

YOROI®
TINEXTA GROUP

Indice di Esposizione Cyber

Nome Cliente

Data di elaborazione: 24/05/2022

Partner tecnologico

Cos'è l'esposizione cyber?

L'esposizione cyber di un'azienda è *l'impronta* digitale lasciata da ogni attività eseguita sulla rete Internet.

Ogni impresa utilizza strumenti digitali per operare nel proprio business, aumentare la propria visibilità sul web, comunicare con clienti e fornitori, gestire le proprie informazioni, condividere dati sulla rete.

Questa costante condivisione porta all'esposizione di una serie di dati, mettendoli potenzialmente a disposizione di chiunque. Sito web, e-mail aziendali, e-mail personali, infrastrutture informatiche esposte su Internet non sempre aggiornate; tutti questi elementi possono diventare di interesse per attori malevoli, criminali informatici interessati a noi o a qualche componente della catena del valore della nostra impresa.

Come è costruito l'indice di esposizione cyber?

L'indice di esposizione cyber è un indicatore che, a partire da una serie di informazioni esposte sulla rete, permette di ottenere maggiore visibilità sulla presenza digitale dell'azienda.

Questo indicatore si compone di tre informazioni, raccolte senza alcuna azione attiva sull'organizzazione e i suoi asset tecnologici, utili a focalizzare **tre viste** rilevanti dal punto di vista della sicurezza informatica aziendale esposta su internet:

Servizi Esposti

I servizi esposti, identificabili come servizi informatici accessibili da Internet, descrivono il perimetro dell'*impronta* digitale dell'azienda sulla rete, comprendono una serie di strumenti tecnologici: per esempio siti web, portali di e-commerce, applicazioni web di gestione di ordini e di condivisione di informazioni con clienti e fornitori; più in generale il servizio esposto è una "finestra" aperta dell'azienda su Internet.

La numerosità di servizi esposti è un indicatore oggettivo, una fotografia della presenza dell'azienda su Internet eseguita in un determinato momento; i sistemi di scansione dei servizi, che operano costantemente, aiutano a definire e mantenere aggiornato un perimetro preciso, sul quale l'attenzione va mantenuta alta.

Vulnerabilità

Le vulnerabilità identificate, sul perimetro dei servizi esposti, evidenziano, tramite una scansione "passiva", le versioni dei servizi esposti che risultano essere vulnerabili rispetto a una base dati di vulnerabilità note, continuamente aggiornata e alimentata.

L'analisi delle vulnerabilità viene eseguita senza alcune interazione con i servizi analizzati, ciò si traduce nell'assenza di ogni attività potenzialmente impattante sulla qualità degli stessi. Le vulnerabilità rilevate sono infatti da considerarsi un primo livello di consapevolezza di esposizione dei propri servizi, cui si consiglia di far seguire, in caso di evidenze significative, un'attività di analisi approfondita.

Nella visualizzazione grafica dell'indice di esposizione cyber, il numero di vulnerabilità dovrebbe essere pari a 0. Un numero alto di vulnerabilità rilevate, può aiutare ad identificare i punti di miglioramento su cui intervenire tempestivamente per ridurre il rischio di diventare vittime di attacchi informatici perpetrati da attori malevoli ai danni dell'aziende.

Data leakage

I data leak sono collezioni di informazioni, disponibili sulla rete, relative a persone e aziende. L'origine di queste collezioni è riconducibile ad attacchi, perpetrati ai danni di diverse organizzazioni, che hanno permesso il furto, da parte di criminali informatici, di informazioni gestite o di proprietà delle organizzazioni colpite. Queste informazioni vengono condivise, arricchite e rese disponibili sulla rete sotto forma di diverse fonti.

Il costante monitoraggio di queste fonti aiuta l'azienda ad identificare se le proprie informazioni sono presenti all'interno questi "data leak", al fine di intervenire tempestivamente e adottare le opportune cautele.

Nella visualizzazione grafica dell'indice di esposizione cyber, il valore di "data leak" dovrebbe essere pari a 0. La presenza di informazioni dell'organizzazione rilevata in uno o più data leak va attentamente valutato in funzione della tipologia di informazione rilevata e, in caso riguardasse credenziali rubate o altri dati sensibili, andranno valutate le opportune contromisure.

Da dove provengono i dati dell'indice di esposizione cyber?

L'indice di esposizione cyber viene estratto a partire da un complesso e innovativo sistema di monitoraggio e analisi delle informazioni che circolano su Internet: la **Threat Intelligence**.

Threat Intelligence è l'insieme organizzato di conoscenza sugli attacchi digitali; essa racchiude informazioni relative alle scansioni continue, effettuate su Internet, integrate dalla costante correlazione di dati e informazioni eseguite a partire da "fonti" informative tecnologiche. Tra le "fonti" della threat Intelligence possiamo annoverare, senza pretesa di esaustività

- Le **Sorgenti OSINT (Open Source Intelligence)**: fonti di libero accesso che possiedono la conoscenza di base sull'andamento di minacce note. Sono fondamentali per comprendere come le minacce evolvono nel tempo e quali indicatori possono aiutarci a ricondurre i singoli data leak ad attacchi noti.
- Le **Private Source**: fonti "proprietarie", racchiudono informazioni relative a minacce individuate e bloccate da opportuni sistemi di scansione e attraverso una rete di sensori opportunamente dislocati e in ascolto sulla rete Internet
- Le **Hidden Sources (deep e dark web)**: fonti "nascoste" ad accesso ristretto, frutto di un costante lavoro di studio e ricerca, racchiudono preziose informazioni relative alle possibili future minacce, come per esempio il monitoraggio delle nuove versioni di malware e le nuove tecniche di attacco.
- Le **Classified Sources**: fonti "classificate", sono informazioni altamente confidenziali, tipicamente ottenute tramite collaborazioni con enti di Intelligence.

Perché è importante avere visibilità dell'esposizione cyber della propria azienda?

Ogni organizzazione è esposta a possibili attacchi informatici. Internet ha introdotto grandi opportunità di ampliamento del business, di visibilità della propria impresa su nuovi mercati; la grande facilità con cui vengono create soluzioni tecnologiche a supporto del business è un incredibile stimo per la crescita delle imprese.

Per contro, questa grande semplicità ha aumentato sensibilmente la quantità di rischi a cui l'impresa è esposta, dagli attacchi cyber, alle truffe telematiche, al furto di identità e molti altri.

La visibilità della propria esposizione cyber aiuta l'organizzazione a prendere coscienza di una serie di possibili vettori di attacco e intervenire tempestivamente per ridurre l'area esposta e correggere eventuali evidenze significativamente rischiose.

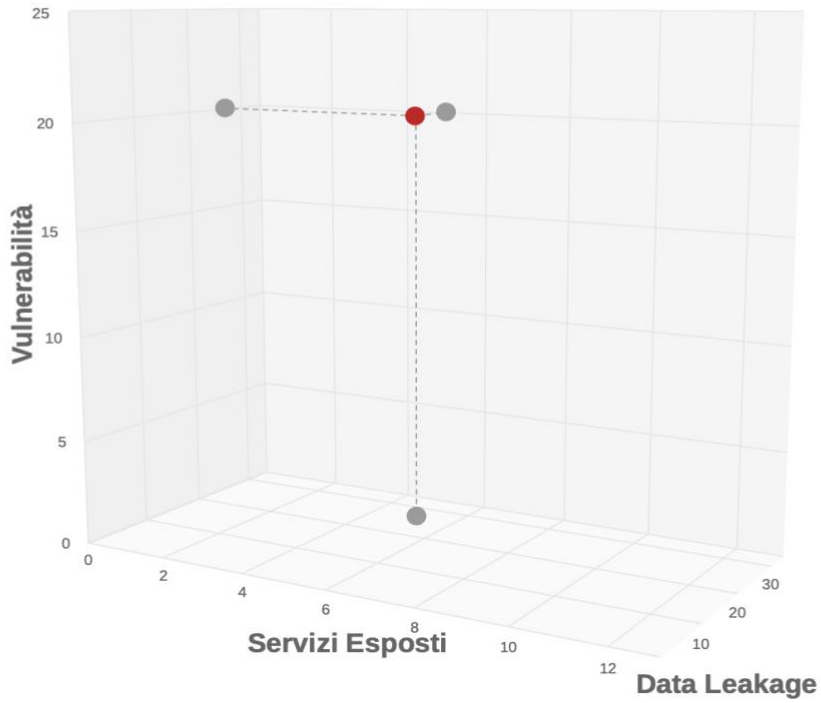
La visualizzazione grafica dell'indice di esposizione cyber, aiuta la lettura di alto livello del risultato: il numero di servizi esposti è un dato oggettivo e non ha una connotazione riferibile alla postura, ma il numero di vulnerabilità e data leak elencati, sono indicatori importanti che devono essere oggetto di attenzione e, ove necessario, rimedio.

DINTEC
CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

CAMERE DI COMMERCIO D'ITALIA

Nome Cliente
Data di elaborazione: 24/05/2022

Indice di Esposizione Cyber



Il punto **ROSSO** rappresenta l'indice di esposizione Cyber dell'azienda.

Servizi Esposti	5
Vulnerabilità	20*
Data Leakage	27*

Servizi Esposti

In questa sezione vengono listati i vari servizi esposti all'esterno (rete Internet) i quali rappresentano appunto, la superficie di attacco esterna. Per ridurre la superficie di attacco, un'azienda dovrebbe analizzare tutti gli IP e servizi esposti all'esterno e ridurre l'accesso solo a quelli strettamente necessari. Per l'individuazione di tali servizi non sono state effettuate scansioni attive.

Host	Porta:	Servizio (versione):
***.197.168.123	22	OpenSSH (7.2p2 Ubuntu 4ubuntu2.10)
Posizione	Porta:	Servizio (versione):
Trieste, it	80	Apache httpd (2.4.18)
Servizi	Porta:	Servizio (versione):
3	443	Apache httpd (2.4.18)

Host	Porta:	Servizio :
***.40.23.136	443	Cloudflare http proxy
Posizione		
Milano, it		
Servizi		
1		

Host	Porta:	Servizio :
***.61.191.142	443	Apache httpd
Posizione		
Trieste, it		
Servizi		
1		

Vulnerabilità

In questa sezione vengono rappresentati i *servizi esposti* con le annesse vulnerabilità di rete riscontrate.

Host : Porta

*****.197.168.123 : 80**

Posizione

Trieste, it

Servizio (versione)

Apache httpd (2.4.18)

Nome:

CVE-2018-1312

Gravità:

CRITICAL

Score:

9.8

Vettore di Attacco:

NETWORK

Data:

26/03/2018 17:29

Descrizione:

In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Host : Porta
*****.197.168.123 : 80**
Posizione
Trieste, it
Servizio (versione)
Apache httpd (2.4.18)

Nome:

CVE-2018-1333

Gravità:

HIGH

Score:

7.5

Vettore di Attacco:

NETWORK

Data:

18/06/2018 20:29

Descrizione:

By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).

Host : Porta
*****.197.168.123 : 443**
Posizione
Trieste, it
Servizio (versione)
Apache httpd (2.4.18)

Nome:

CVE-2018-1312

Gravità:

CRITICAL

Score:

9.8

Vettore di Attacco:

NETWORK

Data:

26/03/2018 17:29

Descrizione:

In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Data Leakage

Questa sezione presenta quali leak contenenti account aziendali sono potenzialmente disponibili ad un attaccante. Nel caso in cui un leak contenga una password, sia essa in chiaro o meno, verrà mostrata l'icona di *Data Leakage* sotto la dicitura *Passwords*. La sorgente di un data leak può avere diverse origini come: collezioni di credenziali, basi di dati esposte o simili .

Account		
*****@customer.com	Sorgente del leak:	**Copy of apollo.io.v5__3___part_1.csv**
	Data di ultima rilevazione:	**23-10-2021 00:00**
	Passwords:	**Hash della Password**

Account		
*****@customer.com	Sorgente del leak:	**Flashbay.com 208k.txt**
	Data di ultima rilevazione:	**05-10-2021 00:00**
	Passwords:	**Hash della Password**

Account		
*****@customer.com	Sorgente del leak:	**United_States.txt.00**
	Data di ultima rilevazione:	**24-09-2021 12:00**
	Passwords:	**Hash della Password**

Account		
*****@customer.com	Sorgente del leak:	**Italy.txt**
	Data di ultima rilevazione:	**24-11-2021 12:00**
	Passwords:	**Password in Chiaro**

IC
InfoCamere

DINTEC
CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

CAMERE DI COMMERCIO D'ITALIA

Partner tecnologico

YOROI
TINEXTA CYBER

Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

TF-CSIRT
Trusted Introducer