UNINDUSTRIA

UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE

ROMA • FROSINONE • LATINA • RIETI • VITERBO

21 GIUGNO 2021

UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

La Trasformazione digitale a portata di Impresa

DIGITAL INNOVATION SHORTCUTS

BUSINESS SECURITY

Cybersecurity: crescere con il digitale, in sicurezza

Mirko Santocono
Fastweb

Leonardo Campanella
InfoAziende

Contesto di riferimento: il business è sempre più digitale, tanti motivi per proteggerlo

Eliminazione accidentale

Guasti

Danni economici e di reputation

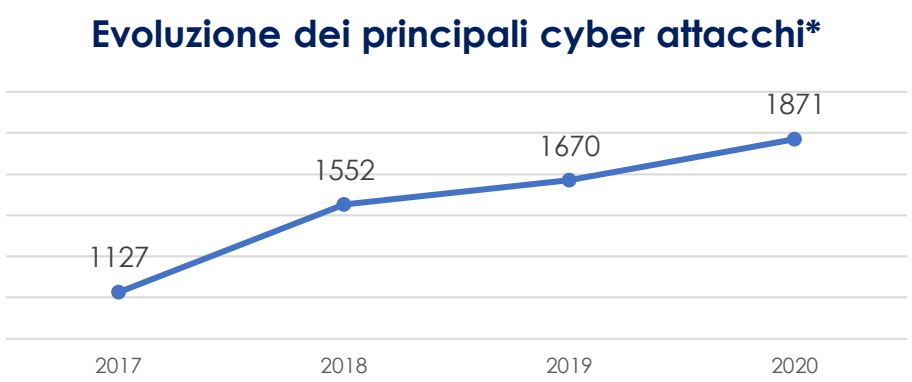
Disastri naturali

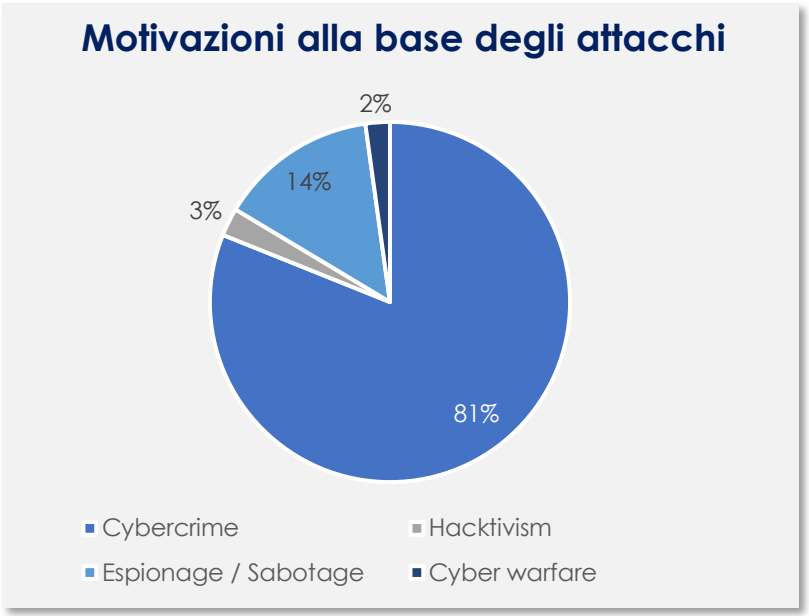
Attacchi informatici

*attacchi noti di particolare gravità avvenuti nel mondo, ovvero che hanno avuto un impatto significativo per le vittime in termini di perdite economiche, di danni alla reputazione, di diffusione di dati sensibili (personali e non), o che comunque prefigurano scenari particolarmente preoccupanti.

Fonte: Clusit, 2021

Contesto di riferimento: i cyber attacchi gravi noti a livello globale sono in crescita





Nel 2020 sono avvenuti 1.871 attacchi gravi resi pubblici, con un incremento del 12% rispetto al 2019 e del + 20% rispetto al 2017. Il numero di attacchi rilevati nel 2020 segna una **differenza del +29% rispetto alla media degli attacchi per anno del triennio precedente** (1.449) e il **cyber crime costituisce il movente principale.**

Gli attacchi del cyber crime sono indirizzati in primo luogo verso le **organizzazioni con meno difese** e si **differenziano adattandosi al tipo di valore che può essere estratto** dall'organizzazione vittima:

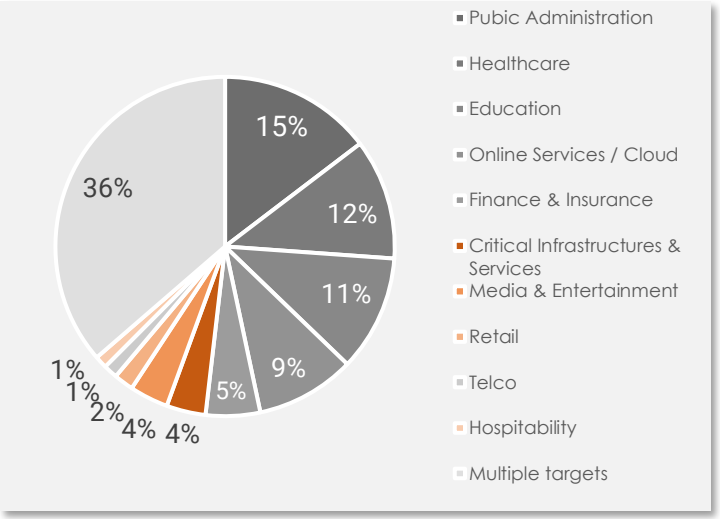
- **Capacità computazionale, da utilizzare ad esempio per l'**estrazione di criptovalute o il *cracking* di credenziali
- **Sfruttamento dell'infrastruttura del cliente per lanciare attacchi verso terzi** (quindi il cliente rischia di essere ritenuto il responsabile dell'attacco e/o di essere coinvolto in indagini della magistratura)
- **Richiesta di riscatto a fronte del blocco dei sistemi** (ransomware)
- **Furto di informazioni per spionaggio industriale / concorrenza sleale** (cyber espionage)
- **Furto di dati personali per rivendita sul mercato nero** (gli acquirenti dei dati poi tipicamente li usano per perpetrare frodi) o **per richiesta di riscatto dietro minaccia di divulgazione**

*attacchi noti di particolare gravità avvenuti nel mondo, ovvero che hanno avuto un impatto significativo per le vittime in termini di perdite economiche, di danni alla reputazione, di diffusione di dati sensibili (personali e non), o che comunque prefigurano scenari particolarmente preoccupanti.

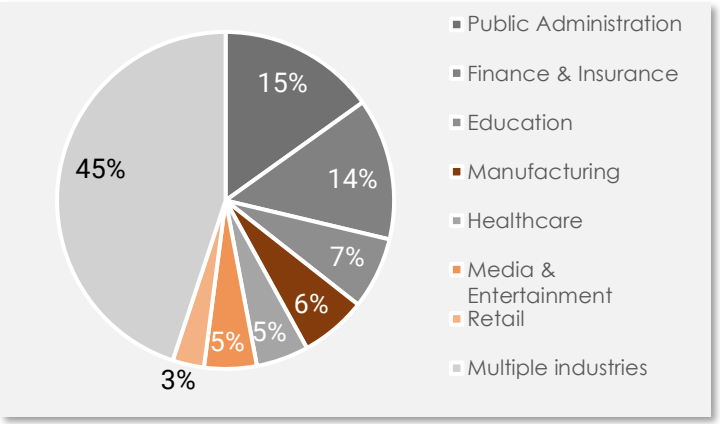
Fonte: Clusit, 2021

Gli attacchi informatici nel settore dell'industria

Distribuzione degli attacchi a livello mondiale[1]



Distribuzione degli attacchi in Italia[2]



Principali evidenze:

- A livello mondiale l'Industria e Servizi è uno dei principali settori vittima di attacchi cibernetici, con un totale cumulato tra i verticali pari all'11% del totale
- In Italia, con il 14% del totale degli attacchi, rappresenta la seconda area **più significativa all'interno dei settori vittima di cyber attack** (a parimerito con il Finance)

Manufacturing[3]

Il 51% dei metodi di attacco più utilizzati sono i **malware «password dumper» e il furto di credenziali** per accedere ai sistemi e rubare i dati aziendali. Un'altra fonte di preoccupazione è l'utilizzo inappropriato da parte dei dipendenti delle proprie credenziali per rubare i dati (13%). Sebbene la maggior parte degli attacchi abbia una motivazione finanziaria è presente anche una consistente quota di attacchi motivati da **cyber espionage (27%).**

Critical infrastructure & services[3]

Tra gli attacchi identificati gli attacchi di **social engineering sono i più diffusi (20%).** Il resto degli attacchi è di natura non identificata per cui si tratta di un settore che deve prestare particolare attenzione agli attacchi innovativi. La motivazione degli attacchi è **prevalentemente finanziaria** con alcuni casi importanti di cyber espionage.

Media & Entertainment[3]

Questo settore è stato esposto prevalentemente ad attacchi di **social engineering, DDoS** e web application breach con motivazione prevalentemente **finanziaria** (94%).

Retail[3]

Gli attacchi contro le **applicazioni di e-commerce** sono di gran lunga le principali cause di violazioni in questo settore (oltre 50%). Poiché le operazioni di vendita si sono ampiamente trasferite online, le violazioni correlate ai device e alle reti dei punti di vendita hanno raggiunto bassissimi livelli. Le motivazioni alla base degli attacchi sono prevalentemente finanziarie, con l'obiettivo di **appropriarsi dei dati relativi alle carte di credito** e ai **metodi di pagamento online (47%).**

Hospitability[3]

Le principali modalità di attacco in questo settore sono malware e hacking utilizzando credenziali rubate. Le motivazioni degli attacchi sono **prevalentemente finanziarie**, in particolare in relazione ai metodi di pagamento (68%).

Fonte:
1 Clusit, 2021
2 Exprivia, 2020
3 Data Breach Investigations Report, Verizon 2020

Come affrontare la sfida?

Tecnologia

Competenze

Investimenti

In House

Servizio gestito in Cloud

Governance

Fonte:
1 Clusit, 2021
2 Exprivia, 2020
3 Data Breach Investigations Report, Verizon 2020

Contesto di riferimento

Esigenza aziendale

- **Aumento del livello di protezione** e sicurezza dei sistemi IT e digitali aziendali, per far fronte alla forte crescita degli attacchi informatici
- Presidio continuativo e **monitoraggio proattivo** della sicurezza informatica
- **Affidabilità e disponibilità** dei dati e applicazioni IT a supporto del core business

Descrizione della soluzione introdotta

Next Generation Firewall

Si tratta di una soluzione di cybersecurity volta a proteggere gli asset digitali delle aziende. Lo use case si basa su un approccio a 360° e composto da tre blocchi base (Installazione; Gestione, Reportistica) basato su apparati di sicurezza Next Generation Firewall.

Web Application Firewall

Si tratta di una soluzione per rilevare ed eliminare una vasta gamma di attacchi e attività dannose, in tempo reale: i sistemi di sicurezza WAF proteggono i servizi WEB e le interazioni tramite API.

Mail Security

Si tratta di un servizio di protezione della posta completamente erogato in Cloud basato su tecnologie di malware detection multi-livello che attraverso un'infrastruttura di Secure Mail Gateway viene instradato il traffico di posta generato o destinato ai mail server del Cliente.

Cosa cambia nel modo di lavorare: l'esperienza di InfoAziende

L'innovazione in azienda

Approccio unificato alla sicurezza, per tutte le esigenze, con capacità di integrazione e protezione dei sistemi mission critical.

L'esternalizzazione dei servizi di sicurezza permette:

- Scalabilità e maggiore flessibilità di gestione
- Flessibilità nella gestione delle risorse: possibilità per i tecnici acquisire Know-how e snellire la gestione di apparati, licenze, vendor, ecc.
- Maggiore focus da parte delle risorse sulla gestione del business aziendale
- Affidabilità di un soggetto terzo esperto e focalizzato sulla sicurezza informatica e che fa questo per mestiere

UNINDUSTRIA

UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE

ROMA • FROSINONE • LATINA • RIETI • VITERBO

10