CyberSecurity – Anticipare le mosse dell'avversario

L'importanza della Cyber Threat Intelligence

La **Cyber Threat Intelligence** riveste un ruolo di primo piano, poiché, talvolta, consente di anticipare le mosse dell'avversario dando modo alle organizzazioni di implementare le contromisure necessarie **prima che si verifichi l'evento analizzato**.

La scelta delle fonti

Risulta essere di fondamentale importanza la scelta delle **giuste sorgenti di intelligence**, identificando le più rilevanti per la propria organizzazione.

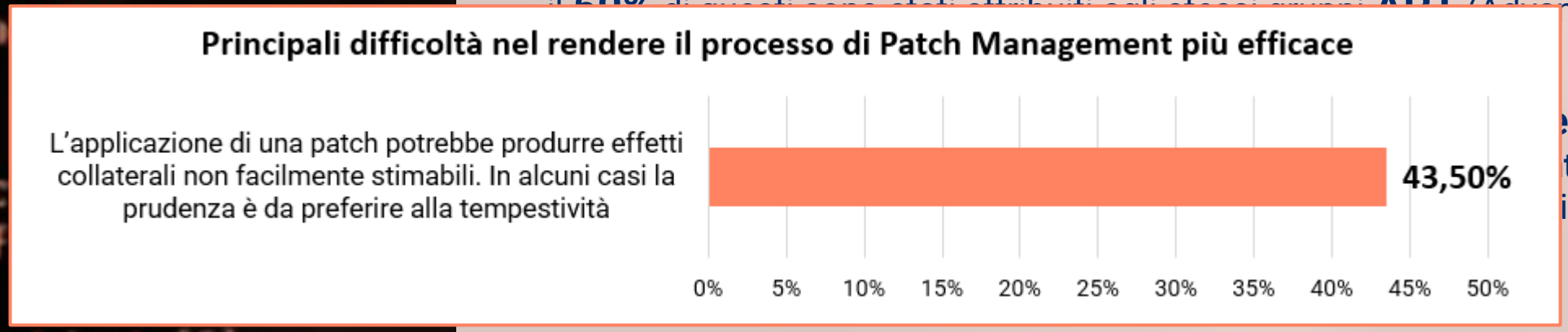
E' necessario focalizzarsi sull'**affidabilità delle fonti** e sulla **qualità delle informazioni** recepite, piuttosto che sulla quantità di queste ultime, anche al fine di evitare il rischio concreto che possa verificarsi un vero e proprio "*sovraccarico di informazioni*", condizione che ricorda lo scrittore **Umberto Eco**, il quale sosteneva che "**troppa informazione equivale a nessuna informazione**".

CyberSecurity – Cosa sta cambiando

Incremento degli attacchi alla Supply Chain

Diversi gruppi criminali sono specializzati nel condurre questo tipo di attacchi: circa il **50%** di questi sono stati attribuiti agli stessi gruppi **APT** (Advanced Persistent

ercettare. Molte
to dei pacchetti
ibuzione legittima



Rafforzamento del processo di Patch Management

Una delle principali minacce cyber che la comunità finanziaria dovrà fronteggiare nei prossimi mesi, è rappresentata dallo sfruttamento delle cosiddette "vulnerabilità **zero day**". Data l'efficacia degli attacchi perpetrati mediante queste vulnerabilità, i criminali informatici trovano una **forte convenienza a investire** nella ricerca delle stesse.

Il CERTFin, nel 2021, ha rilevato un aumento del **206%** del numero di segnalazioni relative a vulnerabilità critiche, rispetto all'anno precedente.

CyberSecurity – Nuovi e Vecchi pattern di Frode

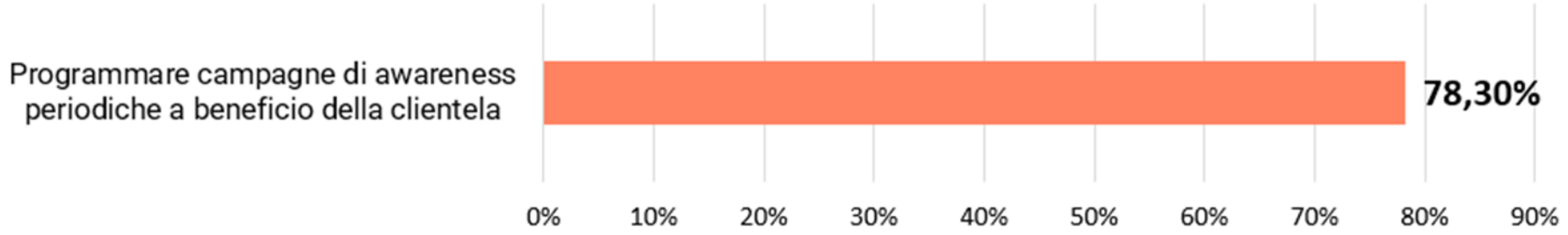
Supremazia delle Tecniche Miste

I risultati delle ultime rilevazioni hanno mostrato una tendenza in aumento degli attacchi che utilizzano le cosiddette «tecniche miste».

Nell'arco del 2020, più del **65%** delle frodi sono state realizzate mediante l'utilizzo di tecniche miste.

Incremento di Mobile Banking Trojan

Strategie che le banche intraprenderanno nel corso del 2022 al fine di prevenire e contrastare efficacemente le frodi informatiche



n congegnati: le
si sono evolute con

malware bancari
di back-end, una
ampliamento

Continua evoluzione del Social Engineering

Sono state osservate campagne sempre **più sofisticate**.

Allo stesso tempo, nel **2021** si è osservato un maggiore impegno da parte dei frodatori nell'elaborare schemi fraudolenti volti ad ingannare il **personale interno bancario.**

CyberSecurity – Resilienza

Il perché…

…I molteplici **fattori evolutivi** quali la digitalizzazione dei nuovi canali di erogazione dei servizi e l'evolversi dell'ecosistema di riferimento (guerre, pandemie, crisi economiche, ….) **modificano dinamicamente il panorama dei rischi.**

…La **crescente esternalizzazione di processi** e la maggiore **articolazione della supply chain** richiedono apposite strategie di gestione della relazione con i fornitori e dei rischi associati

…I **nuovi orientamenti normativi** con requisiti di continuità operativa e resilienza digitale uniformi per tutto il settore finanziario

Il come…

La resilienza digitale necessita di un **approccio coordinato**, pratico ed efficace per **rafforzare la capacità di risposta a cambiamenti continui** ed **eventi imprevisti** attraverso modelli di analisi e predisposizione delle misure di mitigazione e risposta **su tutti i servizi** e anche **per eventi di minore gravità ma maggiore frequenza.**