Platinum Sponsor
snam
Pietro Fiorentini
AON
AIMUW THE FUTURE TOGETHER
Main Sponsor
ASCOPIAVE
centria RETI GAS
estra
INRETE DISTRIBUZIONE ENERGIA
iren
PLASTITALIA high performance fittings
RUBINETTERIE BRESCIANE
SICK Sensor Intelligence.
unareti
WaterTech
Supporter
GREINER
EUROTIS Creatori di soluzioni

RAPPORTO CLUSIT 2021

CYBER SECURITY FONDAMENTALE PER RESILIENZA OPERATIVA DI IMPRESE E ISTITUZIONI

A cura del Comitato Italiano Gas

*In collaborazione con **Emanuele Martinelli**, Energia Media*

Le cronache delle ultime settimane hanno messo l'accento quotidianamente sull'importanza di sistemi di cyber security in grado di proteggere da attacchi che - come ben descrive il rapporto **Clusit** di recente uscita - nel 2021 sono aumentati nel mondo del 10% rispetto all'anno precedente, peraltro con una capacità di produrre danni sempre più ingenti.

Il rapporto, che farà da filo conduttore di questo articolo non tiene conto naturalmente di quanto stia accadendo dall'inizio della guerra della **Russia contro l'Ukraina**; ma non è difficile rilevare che la situazione si fa via via più grave con rischi per ogni tipo di infrastruttura.

Partiamo da qualche dato: da un punto di vista geografico, il **45%** degli attacchi si sono verificati negli **USA**, registrando un leggero **calo rispetto al 2020**; mentre sono cresciuti in Europa (21% contro il 16% del 2020) e in Asia (12%, rispetto al 10% del 2020).

La tendenza è colpire target ben precisi, a partire dal bersaglio governativo/militare in primis, informatico, sanitario e relativo all'l'istruzione in seconda battuta.

In Italia nel 2021 si è rilevata una crescita significativa di malware e botnet, con impatto importante sui server (+58%); ma pure il mobile è stato **sempre più infettato** attraverso SMS o app di messaggistica. In Italia come nel 2020, i settori più colpiti si sono rivelati il Finance/Insurance e la Pubblica Amministrazione; anche se l'aumento più significativo (+18% rispetto al 7% del 2020) arriva dall'industria, il che dovrebbe far alzare le antenne al nostro tessuto produttivo e dei servizi.

Questa personalizzazione negli obiettivi dice di un'evoluzione sempre più sofisticata delle tecniche di attacco - con un significativo moltiplicatore dei danni - sempre più complesse da monitorare e intercettare; il rapporto **Clusit** sottolinea che il problema si fa sempre meno tecnico e più metodologico e specialistico, dal che si deduce come ogni organismo, pubblico o privato che sia, debba necessariamente attrezzarsi adeguatamente per rispondere a una situazione che si fa col tempo sempre più critica.

In merito alle **4 categorie di attacchi**, il **Cybercrime** ha fatto registrare il numero più elevato degli ultimi 11 anni (+16%) come peraltro in crescita sono quelli relativi all'**Information Warfare** (+11,4%); mentre diminuiscono notevolmente quelli riconducibili all'Hacktivism (-58,3%); il Cyber Espionage diminuisce (-17,8%), aveva registrato il punto più alto nel 2020 a causa dello sviluppo di vaccini e cure per il Covid-19.

Sono cresciuti i Malware (+9,7%), che rappresentano il 41% del totale, mentre nuove tecniche sconosciute sono aumentate del 16,4% rispetto al 2020, superando la categoria Vulnerabilità (che peraltro segna un +60%) e Phishing / Social Engineering (-32,1%).

Sale invece la categoria Tecniche Multiple (+19.8%).

Per quanto concerne la gravità degli attacchi per settori il maggior numero è stato registrato nel **Transportation / Storage** (+93,3%), **News / Multimedia** (+60,5%), **Wholesale / Retail** (+51,9%), **Gov / Mil / LE** (+36,4%), **Hospitability** (+36,4%), seguite da **Professional / Scientific / Technical** (+26,2%) ed **Healthcare** (+24,8%).

L'ambito Energy e Utility è compreso negli Other Services (+66,7%), e gli si attribuisce un 2% di crescita complessivo.

Il rapporto Clusit 2021 analizza anche l'impatto critico degli attacchi classificando in **Alto** (36%), **Medio** (32%) e **Basso** (19%) il livello; in termini di **Severity**, nel 2020 gli attacchi con effetti molto gravi (High) sono stati il 47% (36% nel 2020), quelli devastanti (Critical) rappresentano il 32% (contro il 14% del 2020), di impatto significativo (Medium) il 19% (32% nel 2020) mentre quelli con impatto basso solo il 2% (19% nel 2020).

Un quadro a dir poco impressionante che ben dice della gravità del momento, un fatto che deve destare preoccupazione e che denota peraltro un cambio di strategia degli attaccanti.

Ed è la categoria Government ad aver subito il maggior numero di attacchi critici, che significa quanto il livello di tensione tra Paesi e tra privati e istituzioni si stia alzando.

La situazione in Italia

Per quanto concerne il nostro Paese, anche quest'anno **la collaborazione tra Clusit e il Security Operations Center** (SOC) di Fastweb ha dato i suoi frutti.

Dal campione analizzato si è potuto constatare che i maggiori investimenti in security originati da consapevolezza sul tema da parte delle aziende hanno portato a una miglior contrapposizione ed efficacia delle misure di difesa.

La crescita del digitale diffuso **ha in qualche modo costretto gli operatori a un cambio di passo**.

Nella rete di 6,5 milioni di indirizzi IP di Fastweb si sono registrati 42 milioni di eventi da ricondurre alla sicurezza con un aumento del 16% rispetto al 2020. L'aumento più rilevante è stato ai server (+58%) attraverso malware e botnet, soprattutto quelli ospitati in Europa rispetto a quelli residenti negli USA; questo perché si stanno moltiplicando gli investimenti in Data Center realizzati fisicamente nel vecchio continente.

Gli attaccanti hanno utilizzato in particolare **Andromeda**, una piattaforma in grado di distribuire circa **80 famiglie di malware** (tra cui ransomware, trojan bancari, robot spam, malware antifrode e altro ancora).

In tale contesto il Sistema Informativo Nazionale per il Contrasto al Cyber Crime (C.N.A.I.P.I.C.) **nel 2021 ha gestito 5509 attacchi informatici** di un certo peso in merito a servizi informatici di sistemi istituzionali, infrastrutture critiche informatizzate di interesse nazionale e regionale, e grandi imprese; **in questo contesto ha inviato 110.880 alert di sicurezza**.

Nel complesso stati l'anno scorso 256 gli eventi ransomware gestiti (contro i 220 del 2020), di cui 61 contro Infrastrutture Critiche (IC), Operatori di Servizi Essenziali (OSE) e Piccole Amministrazioni Locali (PAL); oltre a 195 attacchi ad aziende.

C'è un fatto da tenere conto, di cui si accenna spesso nel rapporto e a più livelli: il problema si fa meno tecnico, più metodologico e sempre più specialistico.

Nelle conclusioni del capitolo del Rapporto dedicato all'email security in Italia, si sottolinea che gli attacchi di phishing che puntano al furto di credenziali rappresentano un pericolo concreto e in crescita.

Sottolinea Rodolfo Saccani di Libraesva: "*La compromissione di account aziendali rappresenta il primo passo per una serie di attività illecite quali la distribuzione di malware e ransomware dall'interno dell'azienda stessa (bypassando quindi la protezione perimetrale), il furto di informazioni, l'estorsione, lo spionaggio industriale e l'utilizzo delle infrastrutture aziendali come trampolino per ulteriori attacchi verso altre organizzazioni.*

Ogni cosa ha un valore sul mercato del dark web.

Le credenziali, i contenuti delle mail-box, gli accessi ad infrastrutture aziendali vengono venduti e acquistati in tempi brevissimi, spesso più volte, portando in breve tempo una varietà e una molteplicità di attori malevoli all'interno della propria organizzazione.

Preso atto del fatto che le minacce si fanno più subdole e che le tecniche di attacco evolvono in direzioni più difficili da monitorare, da quantificare e anche da intercettare, è opportuno che le organizzazioni restino al passo con l'evoluzione delle tecniche di attacco, le quali seguono una naturale evoluzione verso lo sfruttamento dei punti di ingresso più deboli, inclusi gli individui."

Aprirsi alla tecnologia

Cloud, AI e Machine Learning sono entrati prepotentemente in ogni processo 4.0, e al tempo stesso operano in termini di difesa da attacchi cyber.

L'Intelligenza Artificiale che può dare oggi un contributo fondamentale per ridurre i danni nel caso in cui una azienda sia attaccata, così modelli di Machine Learning controllare attività di autenticazione e accesso di un utente, i download, gli upload, i data transfer e molti altri parametri.

Modelli che imparano attingendo dall'attività di ciascun utente, che rilevano comportamenti anomali, prevenendo azioni automatiche in base alla effettiva rischiosità dell'operazione.

Alcune strumenti d'Intelligenza Artificiale applicabili alla cyber security analizzano blog, siti web, discussioni, mailing list, report, security advisory, ricavando ed elaborando contenuti rilevanti per la cyber security stessa; utilizzando per esempio il Content Analytics con l'obiettivo di estrarre informazioni e indicatori scritti in lingue diverse, a supporto di decisioni e azioni delle diverse figure coinvolte nella cyber security aziendale.

Al tempo stesso se parliamo di intelligenza artificiale, chi attacca con deep fake sarà sempre più in grado di sfruttarla per imitare le attività umane così da perfezionare gli attacchi basati sul social engineering; tra i più allarmanti vi è sicuramente quello relativo agli attacchi di tipo impersonation - in tempo reale su applicazioni vocali e video - che potrebbero permettere ai cybercriminali di superare eventuali riconoscimenti biometrici, ponendo sfide sempre più complesse per garantire l'autenticazione degli utenti in sicurezza.

Trasformare l'elemento umano da vulnerabilità a sensore

È molto complesso rilevare la componente degli attacchi cyber non individuabili attraverso i presidi di sicurezza tecnologici ma attraverso l'elemento umano; la formazione tradizionale si rivela spesso inefficaci, perché sporadica e con scarso e reale coinvolgimento diretto degli interessati.

Un aspetto fondamentale della security awareness è la capacità di abilitare il meccanismo "**human as a security sensor**", in cui è l'utente consapevole a individuare tentativi di truffe basate sull'ingegneria sociale, che avrebbero altrimenti una possibilità scarsa, se non nulla, di essere intercettate con contromisure tecniche di sicurezza.

Servono comunicazione, campagne mirate e continuità nella formazione: da questo dipende anche la tutela del valore di un'azienda, qualunque sia il proprio comparto di riferimento.

I consigli degli amministratori di sistema

Il rapporto Clusit riporta il risultato di interviste a 732 amministratori di sistema di diverse aziende e di tutto il mondo che rappresentano il cuore dell'IT all'interno delle diverse organizzazioni.

Tra i punti messi in evidenza rileviamo la rapida evoluzione delle minacce informatiche ed ammette che il lavoro a distanza ha distolto l'attenzione dalle attività di sicurezza.

È stata quindi stilata questa breve guida per essere tutti più protetti e sicuri.

- *Non pubblicare nulla online che non indosseresti su una maglietta quando il CEO è in visita in ufficio.*
- *Mantieni aggiornato il tuo antivirus e usa la VPN quando lavori sulla rete aziendale.*
- *Non visitare siti Web ingannevoli quando sei al lavoro!*
- *Proteggi il tuo equilibrio tra lavoro e vita privata e prenditi il tempo necessario per quest'ultima.*
- *Conta fino a 10 prima di premere "Invia".*
- *Non cadere vittima di email sospette: se sembra troppo bello per essere vero, è sicuramente una truffa.*
- *Non rispondere a tutti nelle email di gruppo.*
- *Nessuno chiederà mai i dati della tua carta di credito per mostrarti le foto del gatto.*
- *Leggi attentamente cosa dice la finestra di dialogo, non dare mai nulla per scontato.*
- *Usa una password diversa per ogni cosa.*

Incorporare la Cybersecurity nelle strategie di Resilienza Operativa

Chiudiamo questo contributo con l'accento che il **Rapporto Clusit mette sulla Resilienza Operativa** in un momento storico in cui, in particolar modo per chi si occupa di servizi di pubblica utilità, più fattori concorrono (pandemia, guerra, prezzi dell'energia) a dover mettere l'accento su questo fondamentale aspetto.

In ogni organizzazione diventa fondamentale implementare sistemi di gestione di **Risk Management, Business Continuity & Cybersecurity** in modo tale che le persone, i processi e i sistemi informativi possano anticipare, prevenire, rispondere/recuperare e adattarsi per far fronte alle mutevoli condizioni secondo un approccio risk & resilience-based.

Questo per ridurre al minimo l'impatto di un'interruzione sugli stakeholder esterni e sull'economia in generale, sapere dove si trovano le vulnerabilità della propria organizzazione e sviluppare quegli elementi fondamentali (Resilienza Informatica, Aziendale, di Terze Parti e Tecnologica) che contribuiscono ad una ripresa più rapida dell'organizzazione, riducendo al minimo i danni.

Comprendere e gestire la propensione al rischio dell'organizzazione, o la tolleranza per una varietà di rischi a cui è esposta è fondamentale per mantenere i servizi aziendali in funzione durante qualsiasi tipo di evento; il che implica una piena governance dei processi, un cambiamento tecnologico per migliorare la fase di recupero, e un cambiamento culturale per incorporare la Resilienza Operativa all'interno dell'organizzazione stessa.

Ribaltando il problema in opportunità, la **Cybersecurity** dovrebbe essere utilizzata per migliorare la **Resilienza Operativa complessiva** e, al contempo, rafforzare le tradizionali capacità di Business Continuity.

Le buone pratiche di Cybersecurity dovrebbero permeare tutto ciò che riguarda la tecnologia in un'azienda considerando come le policy, le persone e i processi siano strettamente collegati tra loro. Creando una cultura della consapevolezza informatica, da garantire all'utente finale, attraverso comunicazione e formazione.

In tutto questo il coinvolgimento del Top Management è fondamentale, perché il tema impatta sempre più col valore dell'azienda.

Diventa fondamentale analizzare in profondità il livello della propria Cybersecurity in termini di asset digitali, valore aziendale da proteggere e potenziali attacchi hacker da respingere, misurando gli impatti di eventi cyber sui processi/servizi critici tenendo in considerazione la risk tolerance definita dall'organizzazione.

"*Solo attraverso una sinergica e strutturata interazione dei principi di Risk Management, Business Continuity e Cybersecurity - rileva Federica Maria Rita Livelli, tra i maggiori esperti sul tema - sarà possibile garantire la governance e la compliance, rendendo l'organizzazione agile, anti-fragile, adattiva e in grado di garantire la Resilienza Operativa, superando i limiti di un approccio per silos e riprogettando la struttura interna, il modus operandi e pensandi dell'organizzazione stessa.*

Un piano di Business Continuity (BCP) garantirà il ripristino della funzionalità dei sistemi di un'organizzazione; le misure di Cyber-security proteggeranno l'organizzazione; i Piani di Disaster Recovery (DRP) consentiranno una risposta efficace agli inevitabili incidenti informatici. Inoltre, tutti nell'organizzazione dovranno essere sempre più consapevoli del ruolo importante da svolgere in termini di Cybersecurity, in quanto tale ruolo non potrà essere delegato unicamente a un team di professionisti IT."

AGGIORNAMENTI SUGLI SVILUPPI DEL PROGRAMMA SARANNO FORNITI NELLE PROSSIME NEWSLETTER.

A CHI INTERESSA

- *AZIENDE DI TRASPORTO, DISTRIBUZIONE E VENDITA GAS, ELETTRICITÀ, ACQUA*
- *AZIENDE DEL SETTORE ICT E TELECOMUNICAZIONI*
- *FABBRICANTI DI APPARECCHI UTILIZZATORI, ACCESSORI, COMPONENTI E STRUMENTI*
- *AZIENDE COSTRUTTRICI DI IMPIANTI*
- *PROGETTISTI, CONSULENTI AZIENDALI*
- *ISTITUZIONI ED ENTI DI RICERCA*

Forum UNI CIG 2022 i temi trattati:

16 giugno: L'impegno per la sicurezza nel sistema gas nazionale

22 settembre: Sessione 1: Quantificazione e riduzione delle emissioni di metano
Bologna c/o Hotel Carlton Sessione 2: Smart meter & smart grids

17 novembre: Innovazione e ricerca nel settore multi-gas per una transizione energetica sostenibile