Anno 2 / Numero 4
2021

CYBER MAGAZINE

In questo numero:

Sanità nel mirino:
i cyber rischi e le possibili contromisure

L'incidente informatico:
come riconoscerlo e prevenirlo

Cinque buone abitudini per le aziende per minimizzare i rischi di ransomware

ASSINTEL CYBER SECURITY

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

INDICE

L'editoriale del Presidente Assintel

Paola Generali

L'Europa di fronte alla cybersecurity ha un atteggiamento simile a quello del calzolaio che cammina con le scarpe rotte: l'80% delle aziende europee è vittima di almeno un incidente di sicurezza informatica all'anno, dimostrando davvero poca conoscenza sul tema. Ma, parallelamente, proprio alcuni dei principali ricercatori e operatori di cybersecurity più innovativi al mondo sono europei.
Questo dualismo merita una particolare attenzione, perché può essere lo spunto per mettere a fattor comune delle risorse esistenti ed estendere sempre di più la "cyber-evangelizzazione" fra le imprese. Soprattutto se si tratta di MPMI, che restano tradizionalmente più scoperte, per risorse disponibili e cultura aziendale.

In questo contesto, risalta positivamente l'iniziativa europea Cyberwatching.eu, che – come ci spiegano i colleghi della European DIGITAL SME Alliance – fornisce dei tool di analisi e di intervento proprio sui temi della sicurezza informatica e della privacy. Si parte da un'autovalutazione, che attesta con un certificato il superamento del livello basic di consapevolezza e competenze, si prosegue con una sorta di "termometro" che indica il proprio rischio legato alla compliance con il GDPR, ed infine si può accedere a risorse gratuite a livello informativo e formativo. La possibile chiusura del cerchio è un marketplace dedicato, che permette un incontro fra offerta e domanda di soluzioni digitali per la cybersecurity. Uno spunto per riflettere su come sia utile fare sistema, al di là dei particolarismi, con l'obiettivo comune di creare una cultura condivisa che agevoli la crescita digitale nella nostra casa comune europea. Questo numero del Magazine affronta anche questa tematica. Buona lettura.

Sanità nel mirino: i cyber rischi e le possibili contromisure

di ***Pierguido Iezzi***

L'emergenza post pandemia da COVID-19 ha messo sotto pressione le strutture sanitarie. Oltre all'attività primaria di cura dei pazienti, il nuovo scenario informatico e sociale ha creato i presupposti per nuovi rischi, nuove minacce e schemi offensivi che mettono nel mirino proprio l'Healthcare.

I rischi da questo punto di vista coinvolgono principalmente l'asset di maggiore valore contenuto nei sistemi informatici delle strutture sanitarie, ovvero i dati.

Perché i sistemi informatici sanitari sono così interessanti per i threat actor?

I vantaggi di un sistema informativo condiviso che contenga i dati dei pazienti sono ovvi: una più rapida fruizione dei dati, risparmi dal punto di vista economico e burocratico, e uno snellimento delle procedure. La digitalizzazione di questi dati crea però le condizioni ideali per possibili attacchi hacker.

I principali rischi per i sistemi informatici sanitari

Dal punto di vista pratico quali sono i rischi e le minacce principali da tenere in considerazione in questo specifico ambito?

Il problema "ransomware"

Nell'ultimo periodo diverse strutture sanitarie di altri Paesi sono finite nel mirino di organizzazioni criminali specializzate nell'uso di ransomware. Con particolare riferimento alle strutture private degli Stati Uniti, i threat actor hanno notato una maggiore inclinazione al pagamento del riscatto rispetto ad altri operatori in settori diversi.

Il ricorso obbligatorio (e spesso implementato in maniera troppo rapida) di sistemi di tracciamento o trattamento a distanza, l'uso di applicazioni e servizi digitali anche di ricerca per gestire l'emergenza e la campagna vaccinale da COVID-19 non hanno fatto altro che aumentare la superficie utile d'attacco. Sono proprio questi elementi ad aver costretto la CISA, il principale organismo statunitense per quanto concerne la cybersecurity, a emanare un avviso a tutto il settore dell'healthcare.

Nel contesto dei data breach del settore sanitario, avvenuti fra gennaio 2020 e febbraio 2021, il 55% dei casi è avvenuto proprio a causa di un attacco ransomware. E durante il periodo dell'offensiva, l'accesso agli EHR (electronic health records) è stato negato, costringendo in alcuni casi i pazienti a rivolgersi ad altre strutture. La soluzione utilizzata fino a poco fa per questo problema si basava principalmente sulle cyber assicurazioni ma visti i recenti eventi, per alcune strutture diventa obbligatorio implementare sistemi di autenticazione a più fattori e sistemi di endpoint detection and response per ottenere l'accesso a polizze.

Phishing in aumento

Oltre ai rischi dei ransomware, non va trascurato il fattore umano che lascia spesso la porta aperta a offensive di phishing. Come dimostrato da una recente ricerca del team Unit 42 di Palo Alto Network ci sarebbe stato un aumento del 189% dei casi di attacco phishing verso o legati a farmacie e ospedali fra dicembre 2020 e febbraio 2021. Nello stesso lasso di tempo, gli attacchi a tema "vaccino" sono aumentati del 530%.

Questo è un tratto comune delle campagne di phishing: il cambiare tema con uno sguardo sempre rivolto all'attualità per sfruttare ancora di più l'emotività dei destinatari del messaggio (non solo via email ma anche via SMS con la tecnica dello smishing) per ridurre la capacità di critica ragionevole e aumentare il tasso di conversione (ovvero di esecuzione dell'azione richiesta sia essa un click su di un link o il download di un allegato).

Anche in questo caso è importante investire sul Fattore Umano, coinvolgendo le risorse in attività di formazione con corsi e webinar sui temi del phishing. Le tecniche offensive si stanno evolvendo e una conoscenza superficiale della materia può risultare pericolosa.

Vulnerabilità su cloud ed errori di configurazione

I data breach si sono spesso verificati anche per configurazioni troppo sbrigative delle piattaforme e dei servizi su cloud utilizzati dal personale ospedaliero.

L'aumento di richiesta di "telehealth" ovvero cura sanitaria da remoto ha aumentato la gravità del problema.

Il tema fondamentale è uno: l'aumento della superficie d'attacco. La pandemia ha costretto il personale e le strutture ospedaliere a fare ricorso a strumenti innovativi, spesso senza considerare attentamente le possibili ramificazioni dal lato della cybersecurity. Ora è però necessario fissare standard comuni e configurare con attenzione le soluzioni tecnologiche per non mettere a rischio i dati degli utenti.

Un sondaggio di Infoblox proprio sul punto ci ha restituito dei valori allarmanti: il 53% degli operatori sanitari coinvolti ha dichiarato che la propria struttura ha avuto casi di data breach su cloud nei 12 mesi precedenti. Uno degli esempi più famosi è il recente caso di un database su cloud non protetto che conteneva i dati di 3,1 milioni di pazienti (nel contesto di un software di gestione ospedaliera).

Ecco perché anche le strutture sanitarie devono rivalutare il proprio approccio al tema della cybersecurity, riducendo il rischio umano attraverso la formazione e ricostruendo le proprie fondamenta a partire dai 3 pilastri della sicurezza predittiva, preventiva e proattiva.

Non abbassiamo la guardia!

Il 67% degli italiani che lavora nella security è sopraffatto emotivamente dalle minacce IT che deve gestire

Uno studio di Trend Micro rivela i costi umani all'interno dei Security Operation Center

di ***Trend Micro***

Il 67% dei professionisti italiani che lavora in un Security Operation Center (SOC) o nell'IT, è emotivamente colpito dal dover gestire e affrontare le minacce IT e i livelli di stress influiscono negativamente sulla qualità della vita fuori dal luogo di lavoro. Il dato emerge da "SECURITY OPERATIONS ON THE BACKFOOT: How poor tooling is taking its toll on security analysts", l'ultima ricerca di Trend Micro, leader globale di cybersecurity.

Lo studio rivela anche che il 51% del campione è sopraffatto dal volume di alert che riceve, mentre il 34% non ha fiducia nelle proprie tecnologie, che dovrebbero mettere in ordine di priorità le minacce, e spende il 26% del proprio tempo a risolvere falsi positivi.

"I professionisti che lavorano all'interno dei Security Operation Center svolgono un ruolo cruciale nella lotta alle minacce cyber poiché si trovano in prima linea a dover gestire gli attacchi per mantenere le proprie organizzazioni al sicuro da potenziali catastrofi, ma le pressioni a volte possono avere un alto costo personale". Ha affermato Salvatore Marcis, Technical Director di Trend Micro Italia. "Le organizzazioni devono preservare il proprio organico e implementare delle piattaforme di rilevamento e risposta più sofisticate che siano in grado di correlare e mettere in ordine di priorità gli alert. Questo non solo aumenterà il grado generale di protezione ma anche la produttività e i livelli di soddisfazione degli analisti di cybersecurity".

La ricerca rivela che molti responsabili SOC non riescono a rilassarsi e sono irritabili in famiglia e con gli amici. Sul luogo di lavoro oltre il 44% del campione ha ammesso di aver dovuto spegnere gli alert e di essersi allontanato dal computer (39%) per non essere sopraffatto emotivamente del tutto. Il 54% degli intervistati spera anche che in queste occasioni intervenga un collega, il 42% ignora gli alert.

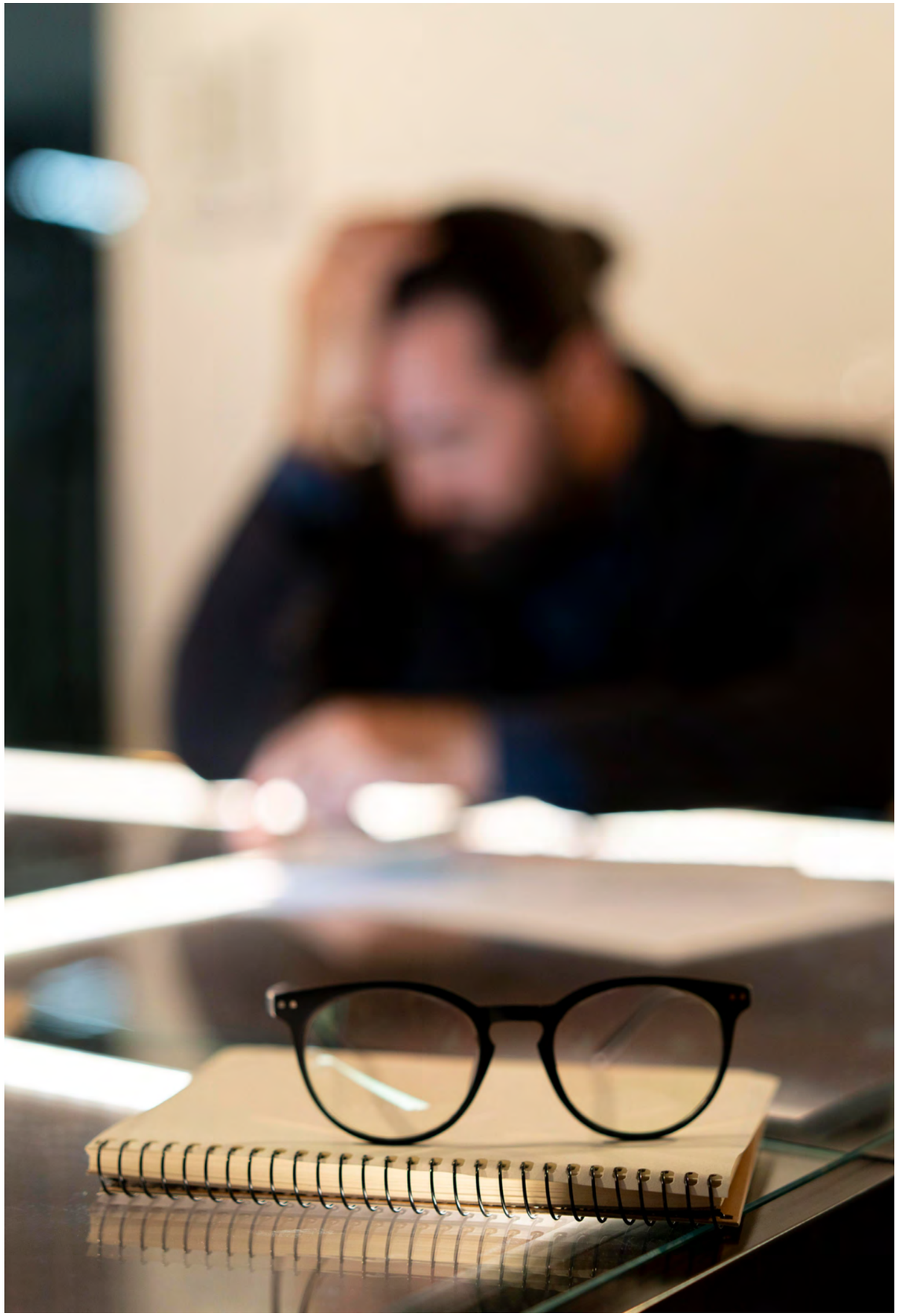
I team che lavorano nei settori real estate, legale, retail e sanità sono quelli maggiormente sommersi dal lavoro. Ad alzare i livelli di stress, il fatto che solo il 53% del campione dichiari di poter contare sul supporto della dirigenza e che il 69% si aspetta o sia già alle prese con una violazione.

I risultati della ricerca di Trend Micro sono corroborati da un recente studio di Forrester[1] che afferma che "i team di IT security sono sotto organico in caso di incident response. I Security Operation Center hanno bisogno di un metodo di detection e response più efficace, ad esempio VisionOne XDR, completamente diverso da quelli presenti ora sul mercato".

Metodologia e campione della ricerca

La ricerca, commissionata da Trend Micro a Sapio Research, ha coinvolto 2.303 IT security decision maker in 21 Paesi, provenienti da aziende con più di 250 dipendenti. In Italia il campione è stato di 100 intervistati.

1 Allie Mellen, Adapt Or Die: XDR Is On A Collision Course With SIEM And SOAR (Forrester, 2021)



L'incidente informatico: come riconoscerlo e prevenirlo

di ***Davide Rapallino***

Nel caso in cui una società venga colpita da un attacco informatico, l'evento viene spesso definito come data breach o incidente di sicurezza delle informazioni.

Ma sono la stessa cosa?

No. I due termini possono sembrare simili ma è molto importante imparare a distinguerli in considerazione del fatto che per le aziende possono derivare differenti obblighi normativi.

In questo articolo cercheremo di spiegarvi come saper distinguere questi due eventi.

Prima di tutto... in cosa consistono?

Incidente di sicurezza delle informazioni.

È un evento indesiderato o imprevisto che può essere causato da un evento naturale, attacchi e violazioni ed ha una significativa probabilità di:

- compromettere le operazioni aziendali;
- minacciare la riservatezza, integrità e disponibilità del patrimonio informativo aziendale.

A titolo esemplificativo possono essere qualificati come incidenti di sicurezza:

1. accesso a reti, sistemi, applicazioni di proprietà della società da parte di personale non autorizzato;
2. blackout che condiziona l'operatività dei sistemi informatici;
3. violazione delle politiche di sicurezza aziendali.

Data breach

Mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali.

Questo perché un incidente di sicurezza include, oltre gli eventi causati da attacchi effettuati dall'esterno, anche incidenti derivanti dal trattamento interno che violano i principi di sicurezza.

La violazione di sicurezza dei dati personali (cd. data breach), dunque, è una particolare tipologia di incidenti di sicurezza che ha ad oggetto informazioni di natura personale e può pertanto comportare un rischio elevato per i diritti e le libertà delle persone fisiche.

Per tale motivo, a differenza di un incidente di sicurezza, tale violazione deve essere notificata al Garante per la protezione dei dati personali come disposto dagli artt. 33 e 34 del Regolamento generale per la protezione dei dati personali (GDPR).

Alcuni esempi di data breach possono essere:

- un accesso non autorizzato ad un sistema nel quale sono conservati dati personali;
- un attacco ransomware che ha reso inaccessibili alcuni dati personali.

Con il sempre maggior numero di persone che lavorano da remoto, negli ultimi anni sono aumentate vertiginosamente le violazioni di dati personali.
In base al Data Breach Investigations Report di Verizon Business gli attacchi di phishing nel 2020 sono aumentati dell'11%, mentre quelli che utilizzano ransomware del 6%. L'85% delle violazioni è stato determinato da una componente umana e oltre l'80% è stato scoperto esternamente all'organizzazione.

Come posso dunque determinare se un evento è un incidente di sicurezza o un data breach?

L'elemento che ci permette di differenziare i due eventi è la tipologia di dati coinvolti in quanto se sono interessati i dati personali, l'evento sarà classificato come data breach mentre in tutti gli altri casi rimarrà un incidente di sicurezza.

Occorre sottolineare che spesso un data breach inizia come un incidente di sicurezza e solo in seguito passa al livello successivo.

Quindi la domanda successiva sorge spontanea.

Come prevenire e gestire un incidente di sicurezza?

Le aziende, considerando l'incremento degli attacchi informatici, devono quindi essere pronte a prevenire e gestire un incidente informatico impostando un efficace piano di Incident Response che viene definito come la capacità operativa di identificare, preparare e rispondere agli incidenti di sicurezza.

In particolare, questo processo si avvale di procedure e linee guida che possono essere raggruppate in 6 fasi:

1. **Preparazione**: consistente nella stesura di un piano e nella definizione delle procedure operative.
2. **Rilevamento e classificazione** degli incidenti di sicurezza in base al livello di gravità e all'elemento scatenante;
3. **Contenimento dell'attacco** per minimizzarne gli effetti;
4. **Raccolta e analisi** delle prove per contenere efficacemente una violazione e a concentrarsi su attività di risanamento;
5. **Ripristino**: indicare le misure atte a garantire che le normali operazioni e le procedure volte a prevenire incidenti futuri vengano ripristinate;
6. **Valutazione e adeguamento**: inserire nel piano i risultati di quanto appreso dall'incidente per migliorare le metriche, i controlli e le pratiche di sicurezza informatica.

In conclusione, il processo di Incident Response, oltre ad essere uno strumento essenziale per prevenire e gestire gli incidenti di sicurezza, costituisce un tassello del più generale piano di Business Continuity che serve a garantire continuità alle attività aziendali a fronte di una qualsiasi tipologia di evento e a prevenirne una possibile interruzione.

Perché non cedere alle richieste di riscatto dei cybercriminali

di ***Riccardo Paglia***

I ransomware continuano a creare danni rilevanti ad aziende di tutto il mondo. E a fronte dell'evoluzione dello schema offensivo, un numero sempre maggiore di vittime decide di pagare il riscatto per chiudere la questione riducendo le perdite. Ma è davvero la strada maestra da percorrere?

Cos'è un ransomware?

I ransomware sono malware che hanno l'obiettivo di cifrare e sottrarre dati sensibili alla macchina, alla rete o al sistema informatico colpito. Dopo che i dati sono stati resi inservibili, viene lasciata una nota di riscatto che indica la cifra da pagare per riottenere accesso alle proprie informazioni attraverso una chiave.

I numeri della questione

Le percentuali non mentono e sono il frutto di un recente studio condotto dal NISC (Neustar International Security Council): il 60% delle vittime di un attacco ransomware decide di pagare il riscatto. Numeri che combaciano sostanzialmente con quelli raccolti da Kaspersky in un simile sondaggio concluso nella primavera del 2021 (in cui la percentuale era del 56% su un campione di 15.000 consumatori).

Sono interessanti anche i dati demografici rispetto ai paganti:

La fascia di popolazione di età compresa fra 35 e 44 anni è stata quella più propensa a pagare (65%).
Tendenze più basse al pagamento si sono invece registrate fra le vittime con età compresa fra 16 e 24 anni (52%).
E solo l'11% delle vittime con età superiore a 55 anni ha deciso di chiudere la questione cedendo all'estorsione dei cyber criminali.

Pagare non significa risolvere

L'aspetto preoccupante è che una percentuale compresa fra il 13 e il 17% (rispettivamente nello studio condotto dal NISC e da Kaspersky) non si è vista restituire i dati anche dopo aver effettuato il pagamento.

E il ripristino dei dati è comunque nella maggior parte dei casi parziale e laborioso dato che solo il 29% delle vittime è riuscito a riavere i propri dati nella loro totalità e integrità.
Questi numeri ci dimostrano che negli ultimi 12 mesi una fascia significativa di consumatori ha deciso di pagare il riscatto per riavere accesso ai propri dati.
Ma pagare non significa necessariamente chiudere la questione, anzi, incoraggia i cyber criminali a continuare sulla stessa falsariga.

Ecco perché è sempre preferibile non pagare: immaginare una scorciatoia, una soluzione rapida all'interno di un contesto così complesso, non è realistico. Il giro d'affari dei ransomware è continuato a crescere anche a seguito del caso Colonial Pipeline e non sembra destinato ad arrestarsi nemmeno a fronte della maggiore attenzione mediatica e giurisdizionale sul fenomeno.

Una tendenza in crescita

Invece che pagare il riscatto e sperare per il meglio, le aziende, gli individui e le organizzazioni a rischio dovrebbero mettere maggiore enfasi sulla prevenzione del rischio ransomware. Spesso la decisione di pagare è motivata dall'assenza di effettive alternative dato che le soluzioni di cyber security attualmente applicate non sono risultate sufficienti nel rilevamento, nella mitigazione e nella prevenzione di questa minaccia.

E questo vale anche per colossi dei settori più disparati, aziende che almeno da un punto di vista teorico dovrebbero disporre delle risorse umane, tecnologiche ed economiche per far fronte alla questione. Il gigante JBS, principale operatore negli Stati Uniti nel settore della macellazione della carne, ha confermato il pagamento di 11 milioni di dollari di riscatto a seguito dell'attacco subito dal ransomware REvil, all'interno di un'offensiva in grado di mettere in ginocchio e bloccare l'intero processo produttivo aziendale.

E aveva pagato anche Colonial Pipeline una cifra pari a 4,4 milioni di dollari, dopo l'attacco che ha fatto notizia anche nel nostro Paese, creando impennate dei prezzi e scene di caos alle stazioni di servizio di diversi Stati USA. Potremmo anche citare il caso di CNA Financial che sempre a maggio si è vista costretta a pagare 40 milioni di dollari di riscatto per riottenere pieno controllo dei propri sistemi informatici.

Se non bisogna pagare, cosa fare?

La statistica e i freddi dati ci dicono che pagare non risolve la situazione, anzi probabilmente l'ha aggravata a livello sistemico. Cosa bisogna fare allora per difendersi dalla minaccia dei ransomware?

È necessario rivalutare nel complesso il proprio approccio alla cybersecurity ricostruendo la propria architettura su 3 pilastri fondamentali:

- Sicurezza Predittiva.
- Sicurezza Preventiva.
- Sicurezza Proattiva.

Questo nella pratica significa valutare il tema della sicurezza nella sua complessità, non limitandosi al proprio perimetro difensivo, ma guardando oltre, rimanendo costantemente aggiornati sullo stato delle minacce esterne, sulle tendenze dell'ultimo periodo e cercando attivamente possibili indicatori che facciano presupporre una violazione dei propri sistemi.

Con un sistema di sicurezza formato da strumenti automatici efficaci, software aggiornati, reti prive di vulnerabilità gravi e un organico composto da persone formate, l'indice di rischiosità dei ransomware scende notevolmente, eliminando alla radice le condizioni necessarie affinché la complessa catena di attacco che culmina con la richiesta di riscatto diventi realtà.

Non abbassiamo la guardia!

Cinque buone abitudini per le aziende per minimizzare i rischi di ransomware

*di **Kaspersky Lab***

I ransomware possono sembrare un problema che riguarda esclusivamente le aziende più grandi e conosciute. In realtà, come dimostrano diversi studi di Kaspersky, sono molte le ragioni per le quali anche le piccole e medie imprese (PMI) dovrebbero esserne a conoscenza e cercare di tutelarsi. Nel 2020 infatti circa il 35% delle PMI è stato colpito da un attacco ransomware, con un costo medio di $183.000: questo dimostra che il trend non dovrebbe essere ignorato.

Lungi dal passare inosservate, le piccole e medie imprese potrebbero risultare addirittura più vulnerabili proprio perché non considerano la sicurezza informatica una priorità rispetto ad altre problematiche aziendali. Tuttavia è importante farsi trovare pronti nell'eventualità di un attacco, soprattutto perché molte semplici abitudini per la sicurezza informatica sono anche utili in generale a garantire processi aziendali più affidabili e sicuri. A questo proposito riportiamo qui alcune misure essenziali e best practice da seguire per le aziende:

Fare regolarmente i backup, non solo una tantum

I backup di sistema dovrebbero essere un processo regolare: è essenziale garantire che siano sempre accessibili e aggiornati. Effettuare sempre nuovi backup e, se possibile, archiviarli su dispositivi che non siano connessi alla rete aziendale. In questo modo i dati rimarranno al sicuro nel caso l'intera rete venga compromessa. Inoltre, è importante fare sempre in modo che in caso di emergenza i backup si possano facilmente recuperare e utilizzare. Questa è un'ottima pratica per ogni situazione, non solo quando si tratta di ransomware. Si tratta di un modo per tornare indietro nel tempo, al momento precedente a qualsiasi incidente che abbia causato la perdita o la corruzione di dati aziendali. Uno dei grandi punti a favore di questo approccio è che l'azienda può continuare a funzionare normalmente, senza interruzioni.

Mai rimandare gli aggiornamenti

Eseguire gli aggiornamenti quando richiesto dal vostro sistema operativo può sembrare una seccatura inutile, specialmente quando si sta svolgendo un lavoro importante o si è di fronte ad una lista lunghissima di email da inviare. Tuttavia, l'esecuzione di un aggiornamento sul sistema operativo o sul software aziendale può fornire informazioni molto importanti circa la sicurezza, nonché le funzionalità che potrebbero semplificare il lavoro che si sta facendo. Invece di vederlo come tempo sprecato, andrebbe utilizzato come momento per sgranchirsi le gambe, riposare gli occhi, prendere qualcosa da bere e tornare al lavoro con rinnovata concentrazione e, soprattutto, con un dispositivo più sicuro.

Continuare a parlare di sicurezza informatica

Sapere è potere quando si tratta di sicurezza online. È importante quindi che le aziende informino i dipendenti della varietà di minacce per la sicurezza informatica a cui potrebbero andare incontro, che si tratti di email di phishing, siti web sospetti o software scaricati da fonti non ufficiali. Dovrebbe essere un processo rilassato e informale, ad esempio attraverso una sessione online di domande libere, accompagnata da immagini e storie vere e coinvolgenti con cui ci si possa identificare. Se è necessario un approccio più formale, si potrebbe prendere in considerazione una formazione interattiva e l'utilizzo di test per garantire che i dipendenti prestino attenzione, in particolare quelli che lavorano con dati sensibili come chi si occupa di contabilità, questioni legali e risorse umane.

Avere cura delle proprie password

Non tutte le password vengono create utilizzando la stessa attenzione. È importante usare chiavi d'accesso complesse per accedere ai servizi aziendali, e utilizzare l'autenticazione a più fattori per fare accesso ai servizi da remoto. Questo è particolarmente importante per servizi aziendali quali ad esempio la contabilità, dove queste precauzioni sono in grado di proteggere dati e denaro da azioni accidentali o intenzionali. Prendiamo il caso in cui venisse smarrito il laptop aziendale. Molte aziende sono preparate all'eventualità di perdere beni fisici, ma è solo attraverso l'uso di password sicure che si può essere certi che i dati rimangano al sicuro se il laptop finisce nelle mani sbagliate.

Sperare per il meglio, prepararsi al peggio

Spesso, quando in azienda, per qualsiasi motivo, si verificano casi di perdita di dati, scoppia il panico e i diversi dipartimenti cercano di stimare come ciò influirà su di loro e sui loro team. In questi casi degli ottimi piani di risposta e di comunicazione possono aiutare a contenere il panico. Andrebbero considerati come una sorta di rifugio e una scorta di rifornimenti contro una futura tempesta, in grado di aiutare l'azienda a resistere alla crisi e, qualora fosse necessario reagire in modo tempestivo, a risparmiare tempo durante i processi decisionali.

E se accadesse il peggio?

I ransomware possono colpire qualsiasi azienda, grande o piccola che sia, ma è importante ricordarsi che il riscatto non andrebbe mai pagato, per nessun motivo. In un primo momento potrebbe sembrare la soluzione migliore e anche l'unica, ma non dà la garanzia di recuperare i dati. Al contrario, incoraggerà i colpevoli a continuare con le loro attività illecite mostrando loro che il crimine paga.

Infatti, secondo quanto emerso da un'indagine di Kaspersky su un campione di 15.000 utenti a livello globale, solo un quarto di coloro che hanno pagato i truffatori ha recuperato i propri dati. La cosa migliore da fare è segnalare l'accaduto alle forze dell'ordine, invece di cedere al ricatto. Altrimenti è possibile cercare online uno strumento di decrittazione come No More Ransom.

Far diventare le buone abitudini parte integrante della giornata, offre diversi benefici con sforzi minimi o nulli. Questo è particolarmente importante per le PMI, per proteggersi da potenziali attacchi informatici e dall'effetto a catena che ciò può avere sulle operazioni quotidiane. Per avere cura dei propri profitti non c'è soluzione migliore di rimanere vigili e attuare comportamenti sicuri.

Cybersecurity Act – Il futuro delle certificazioni europee per la Cyber-Security di prodotti e servizi “ICT”

di ***Riccardo Modena***

Cos’è il Cybersecurity Act?

La Cybersecurity è un tema di rilevante attualità soprattutto nel panorama politico-economico attuale, caratterizzato dal forte impatto delle nuove tecnologie nei processi aziendali, nella nostra società e nel nostro modo di vivere.

In tale contesto l’attività di prevenzione, rilevazione e gestione degli attacchi che provengono dal Cyber-Space diventa un’esigenza irrinunciabile. In questo contesto l’Unione Europea ha pubblicato nell’Aprile 2019 “Regolamento U.E. 2019/881 (…) relativo al ruolo ENISA (…) e alla certificazione della cybersicurezza per le tecnologie dell’informazione e della comunicazione (…)” - meglio conosciuto come Cyber-Security Act – la cui entrata in vigore a tutti gli effetti è prevista per il mese di Giugno 2021, a distanza di due anni dalla sua pubblicazione. Trattandosi di un Regolamento Europeo (quindi una fonte normative sovraordinata rispetto alle leggi nazionali), il Cybersecurity Act è immediatamente recepibile e applicabile in tutti i Paesi Membri, senza necessità di ulteriori interventi legislativi. Il Regolamento Cybersecurity Act rafforza il ruolo di ENISA: tra i nuovi compiti dell’Agenzia vi è infatti quello di fornire ai Paesi Membri consulenza e supporto alla gestione degli attacchi informatici, in cooperazione con i restanti membri dell’Unione Europea.

Oltre a fornire un sostegno concreto e puntuale ai singoli Paesi Membri, ad ENISA spetta un ruolo chiave nella definizione degli schemi per la certificazione di prodotti e servizi “ICT” introdotti dal Cybersecurity Act. Il Cybersecurity Act, sviluppato in coerenza con i principali Standard Internazionali in materia di sicurezza delle informazioni e protezione dei dati personali, è uno degli elementi cardine della nuova strategia dell’Unione Europea in materia di “sicurezza cibernetica”.

Questo Regolamento nasce con l’obiettivo di definire un Framework normativo armonizzato ed applicabile a tutti i Paesi Membri, stimolare la fiducia nell’economia digitale, fornendo alle aziende e ai consumatori informazioni chiare circa il “livello di affidabilità” dei prodotti e dei servizi “ICT”, contrastare il fenomeno del Cyber-Crime, in grado di rallentare la crescita delle aziende e generare sfiducia nei consumatori, attraverso opportune misure di sicurezza, rafforzare la “resilienza” dei Paesi Membri, ovvero la resistenza degli stessi alle principali minacce informatiche. A tale proposito, nel Giugno 2020 si è costituito ufficialmente lo “Stakeholder Cybersecurity Certification Group (di seguito “SCCG”), un gruppo di autorevoli istituzioni europee la cui missione è quella di fornire ad ENISA e alla Commissione Europea il necessario supporto, facilitando la risoluzione di eventuali problemi riguardanti la definizione del Framework di certificazione della Cyber-Security. Nello specifico, l’obiettivo del SCCG è quello di ridurre quanto più possibile la frammentazione degli schemi sviluppati dai singoli Paesi Membri per la certificazione dei prodotti e servizi “ICT”. Attualmente, il SCCG è composto da n. 50 membri provenienti da varie organizzazioni, tra cui: istituzioni accademiche, organizzazioni di consumatori, organismi di certificazione, enti regolatori e preposti allo sviluppo di Standard, aziende, associazioni di categoria e altre organizzazioni associative attive in Europa ed interessate alla certificazione di Cyber-Security. E’ interessante sottolineare che, oltre a supportare ENISA e la Commissione Europea nell’applicazione del Cyber-Security Act, il SSCG è attualmente coinvolto nella la definizione di un nuovo schema di certificazione per i servizi Cloud.

La certificazione di sicurezza dei prodotti e dei servizi digitali

L’esigenza di una revisione della materia deriva dal fatto che molti degli schemi di certificazione attualmente esistenti non sono riconosciuti da tutti i Paesi Membri (e tantomeno dai Paesi non appartenenti all’Unione Europea): ciò obbliga le aziende ad intraprendere diversi processi per l’ottenimento di differenti dichiarazioni di conformità, sostenendo costi significativi per poter offrire i propri prodotti/servizi “ICT” sui mercati transnazionali. Attraverso il Cybersecurity Act, l’Unione Europea mira a facilitare lo scambio di prodotti e servizi “ICT” e al contempo a rafforzare la sicurezza dell’intera catena di approvvigionamento, attraverso l’istituzione di un quadro di regole comuni a tutti i Pasi Membri in grado di disciplinare gli schemi di certificazione su tutto il territorio dell’Unione Europea. A questo proposito è bene specificare che il Cybersecurity Act non istituisce Framework direttamente operativi: questi ultimi, in fase di elaborazione da parte di ENISA per specifiche categorie di prodotti e servizi “ICT”, saranno adottati formalmente dalla Commissione Europea e di conseguenza, resi validi e riconosciuti in tutti i Paesi Membri. Gli schemi di certificazione così adottati sostituiranno progressivamente quelli nazionali, anche se le dichiarazioni di conformità

rilasciate alle aziende non perderanno la loro efficacia e rimarranno validi sino alla loro scadenza naturale. A seguito dell'approvazione di un Framework da parte di ENISA, le aziende potranno richiedere a specifici Enti Certificatori autorizzati la certificazione dei propri prodotti o dei propri servizi "ICT".

Implicazioni aziendali e di mercato

Le implicazioni del Cybersecurity Act, per tutte le realtà di Business che offrono prodotti o servizi "ICT" sono estremamente rilevanti, sotto diversi punti di vista. L'ottenimento di una certificazione rappresenta, infatti, un "plus" d'importanza strategica che consente all'azienda di operare a livello transnazionale ed estendere la propria offerta a tutti i Paesi Membri dell'Unione Europea e ottenere un riconoscimento della sicurezza dei prodotti e dei servizi "ICT" offerti.

La certificazione dei prodotti e dei servizi "ICT" secondo i canoni del Cybersecurity Act prevede infatti di assegnare a questi ultimi un vero e proprio "livello di affidabilità" (di base, sostanziale o elevato) commisurato ai rischi connessi all'uso degli stessi, che è anche un indicatore della capacità di resistere ad eventuali attacchi di natura informatica.
L'acquisizione di una dichiarazione di conformità rappresenta, inoltre, un vero e proprio vantaggio competitivo, in un contesto sociale, politico ed economico sempre più sensibile alla sicurezza delle informazioni, dei dati personali e alla mitigazione dei rischi introdotti dalla sempre più rapida evoluzione delle tecnologie "ICT".
Oltre al miglioramento della reputazione dell'azienda e della percezione della stessa da parte dei propri Stakeholders (es. Clienti, Fornitori, Partner, Pubblica Amministrazione, ecc.), affrontare in modo serio e sistematico un processo di certificazione consente di ottimizzare i processi operativi interni, sistematizzare le misure di sicurezza adottate e coinvolgere il Management nelle principali tematiche di sicurezza delle informazioni e protezione dei dati personali.

Come il "GDPR", che ha introdotto nelle norme in materia di protezione dei dati personali il concetto di "Privacy by Design", anche il Cybersecurity Act disegna un modello basato sul principio di "Security by Design", mettendo la sicurezza cibernetica al centro del processo di sviluppo di prodotti e servizi "ICT".
In quest'ottica, anche i Framework di certificazione elaborati da ENISA dovranno assicurare che prodotti, servizi e processi informatici rispettino una serie di requisiti di sicurezza, puntualmente elencati all'interno dell'Art. 51 del Cybersecurity Act: protezione delle informazioni, dei dati personali e dei servizi "ICT" da accessi, trattamenti o modifiche non autorizzate, cancellazioni, perdite o mancanza di disponibilità; registrazione delle informazioni, dei dati personali o dei servizi acceduti, identificando quali sono stati utilizzati o altrimenti trattati, in quale momento e da chi; verifica che i prodotti (hardware e software) e i servizi "ICT" possano essere mantenuti aggiornati, anche in maniera automatizzata e non contengano vulnerabilità note; ripristino della disponibilità e dell'accesso alle informazioni, ai dati personali e ai servizi "ICT" in modo tempestivo in caso di incidenti, di natura fisica o informatica, in grado di comprometterne la continuità.

Se si considera che ciascuno di questi elementi è già ampiamente trattato da specifici Standard Internazionali (es. ISO 27001 per la sicurezza delle informazioni, ISO 27701 per la protezione dei dati personali, ISO 22301 per la continuità dei processi operativi, ISO 20000 per la qualità dei servizi "ICT", ecc.), l'adeguamento rispetto a queste Best Practices rappresenta il primo passo che ciascuna azienda dovrebbe compiere per non arrivare impreparata al momento della certificazione secondo la prassi del Cybersecurity Act.

Dal perimetro cyber nazionale all'Agenzia Cyber nazionale: a che punto siamo?

di ***Davide Maniscalco***

La configurazione del perimetro nazionale cibernetico è ancora in corso di configurazione e, dopo l'avvicendamento tra il Governo Conte ed il Governo Draghi, continua comunque inesorabile la definizione dell'architettura nazionale di presidio del quinto dominio, a tutela delle infrastrutture strategiche del nostro Paese, da intendersi quali operatori di servizi essenziali (OSE) e fornitori di servizi digitali (FSD).

Va tuttavia detto che la gestazione che ha condotto al Governo Draghi, ha determinato una inevitabile discontinuità che, per certi versi, si è tradotta in una dilatazione del timing per il completamento dell'iter attuativo.

Ed infatti, il primo Dpcm del 30 luglio 2020, n. 131, recante "Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133", pubblicato nella Gazzetta Ufficiale n. 261 del 21 ottobre 2020 (entrata in vigore in data 05/11/2020), ha elencato i criteri di individuazione dei soggetti pubblici e privati inclusi nella cintura di sicurezza.
Successivamente, con separato Dpcm, firmato il 25 novembre è stata predisposta la lista segreta degli oltre 100 soggetti — pubblici e privati — individuati e inclusi nel perimetro.

Nelle successive settimane inoltre, le commissioni Difesa di Camera e Senato, in sede consultiva, davano green light, seppur con rilievi, allo schema del secondo Dpcm recante "notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo l, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza, in attuazione dell'articolo l, comma 3, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133.

Il provvedimento, dopo avere acquisito il parere del Consiglio di Stato, veniva così avviato alla pubblicazione in GURI, che avveniva data 11 giugno 2021 in riferimento al DPCM 14 aprile 2021, n. 81 recante "Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza (Gazzetta Ufficiale n.138 dell'11-6-2021).

A rafforzare l'azione di governo preordinata ad introdurre strumenti di tutela ancora più stringenti contro le escalations di attori stranieri su società che gestiscono assets strategici, venivano emanati i DPCM n. 179 del 18.12.2020 n. 180 del 23.12.2020 (entrambi pubblicati in GU n. 322 del 30.12.2020), rispettivamente recanti "Regolamento per l'individuazione dei beni e dei rapporti di interesse nazionale nei settori di cui all'articolo 4, paragrafo 1, del regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio, del 19 marzo 2019, a norma dell'articolo 2, comma 1-ter, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56" e "Regolamento per l'individuazione degli attivi di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, a norma dell'articolo 2, comma 1, del decreto-legge 15 marzo 2012, n. 21, convertito, con

modificazioni, dalla legge 11 maggio 2012, n. 56", entrambi destinati ad estendere il potere di veto del Presidente del Consiglio dei Ministri, meglio noto come "Golden Power".

Frattanto, con il Dpr n. 54 del 05 febbraio 2021 (pubblicato in GURI n. 97 del 23 aprile 2021) veniva data attuazione alle disposizioni di cui all'articolo 1, comma 6, lettere a), b), e c) del decreto-legge 21 settembre 2019, n. 105, convertito nella legge n. 133/2019, recante "misure urgenti in materia di perimetro di sicurezza nazionale cibernetica e disposizioni riguardanti la disciplina dei poteri speciali nei settori di rilevanza strategica", sullo scrutinio tecnologico sui beni ICT.

A tal proposito giova ricordare che il comma 6 dell'articolo 1, lettere a), b) e c) del succitato decreto-legge demanda a un regolamento – da emanare ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, entro dieci mesi dalla data di entrata in vigore della legge di conversione del decreto-legge – la definizione di procedure, modalità e termini:

- ai quali devono attenersi i pubblici e privati inclusi nel perimetro di sicurezza nazionale cibernetica che intendano procedere all'affidamento di forniture di beni, sistemi e servizi ICT, destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici individuati nell'elenco trasmesso alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico. Si tratta, in particolare, dei beni appartenenti a categorie individuate da un decreto del Presidente del Consiglio dei ministri sulla base di criteri tecnici che dovrà essere emanato entro 10 mesi dall'entrata in vigore della norma di conversione del decreto. Il processo di verifica è effettuato dal Centro di valutazione e certificazione nazionale (CVCN) – istituito presso il Ministero dello sviluppo economico – con riferimento ai soggetti pubblici e privati o dai Centri di valutazione del Ministero della difesa e del Ministero dell'interno per le acquisizioni rispettivamente destinate alle proprie reti, sistemi informativi e servizi informatici. Sono definiti i termini per le fasi di individuazione di test e condizioni per la valutazione dell'oggetto di fornitura e per l'esecuzione dei test, decorsi i quali i soggetti inclusi nel perimetro possono proseguire nella procedura di accertamento.
  Sono stati esclusi gli approvvigionamenti necessari per le attività di prevenzione accertamento e repressione dei reati ed è stato previsto di demandare al decreto attuativo la disciplina dei casi di deroga per le forniture in sede estera;
- con cui i fornitori dei suddetti beni, sistemi e servizi destinati alle reti, ai sistemi e ai servizi rilevanti assicurano al CVCN e ai Centri di valutazione del Ministero della difesa e del Ministero dell'interno, per quanto di rispettiva competenza, la propria collaborazione per l'effettuazione delle attività di test, sostenendone gli oneri;
- con cui il Ministero dello sviluppo economico e alla Presidenza del Consiglio dei Ministri, negli ambiti rispettivamente assegnati loro nel perimetro, svolgono le attività di ispezione e verifica in relazione a quanto previsto dal decreto-legge. In tale contesto, in considerazione delle specificità, le attività di verifica e ispezione riguardanti le reti, sistemi e servizi connessi alla funzione di prevenzione e repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica e alla difesa e sicurezza militare dello Stato, sono svolte, senza nuovi o maggiori oneri a carico della finanza pubblica, dalle strutture specializzate in tema di protezione di reti e sistemi, nonché in tema di prevenzione e contrasto del crimine informatico, delle Amministrazioni da cui dipendono le Forze di polizia e le Forze armate, che ne comunicano gli esiti alla Presidenza del Consiglio dei ministri per i profili di competenza.

Frattanto con nota del 15.06.2021, il Presidente del Consiglio, Mario Draghi, a seguito della proposta formulata dal Comitato interministeriale per la sicurezza della Repubblica, ha firmato, l'aggiornamento dell'elenco dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica.

È stato, così, previsto un allargamento dell'ambito di applicazione del perimetro ad ulteriori soggetti pubblici e privati che, complessivamente, esercitano, attraverso reti, sistemi informativi e servizi informatici, 223 funzioni essenziali dello Stato, ovvero erogano servizi essenziali per il mantenimento di attività civili, sociali o economiche strategiche.

Allo stesso tempo, si è provveduto ad un affinamento di alcune funzioni e servizi essenziali dello Stato già ricompresi nel perimetro.

I soggetti pubblici e privati ulteriormente inclusi nel perimetro saranno conseguentemente notificati dal Dipartimento delle informazioni per la sicurezza ed entro sei mesi saranno tenuti a comunicare le reti, i sistemi informativi ed i servizi informatici che impiegano rispettivamente per l'erogazione delle funzioni e dei servizi essenziali dello Stato inclusi nel perimetro.
Viene dunque innalzato ulteriormente il livello di resilienza cibernetica degli attori maggiormente sensibili ai fini della sicurezza nazionale.
Parallelamente, dal 23 giugno 2021 il perimetro di sicurezza nazionale cibernetica ha iniziato ad essere "operativo" nei confronti dei soggetti pubblici e privati inseriti nella lista originaria.

Questi ultimi sono, quindi, tenuti ad applicare le previste misure di sicurezza e a notificare allo CSIRT italiano gli eventuali incidenti che si dovessero verificare (la lista delle misure di sicurezza e la tassonomia degli incidenti per cui il soggetto è tenuto a notificare sono state pubblicate in allegato al DPCM 81/2021 dell'11 Giugno 2021).

Per permettere una adeguata organizzazione ai soggetti inclusi nel perimetro al fine di ottemperare alle procedure di notifica di incidenti, queste ultime procederanno in via sperimentale fino al 31 Dicembre 2021.

A questo punto, seguendo la roadmap disegnata dalla Presidenza del Consiglio, si attende l'emanazione degli ultimi due Dpcm:

- il terzo afferente alle categorie per le quali sarà necessario effettuare la notifica al Centro di valutazione e certificazione nazionale (CVCN);
- il quarto, relativo ai criteri per l'accreditamento dei laboratori competenti per le verifiche delle

condizioni di sicurezza, atteso in GURI per giugno 2021.

Intanto, in data 8 giugno 2021, veniva pubblicato nella Gazzetta Ufficiale dell'UE il Regolamento (UE) 2021/887 del Parlamento Europeo e del Consiglio del 20 maggio 2021 che istituisce il Centro Europeo di Competenza per la cybersicurezza nell'ambito industriale, tecnologico, della ricerca e della rete dei centri nazionali di coordinamento.

A tal riguardo, è mandatorio l'articolo 6, rubricato "Designazione dei centri nazionali di coordinamento", paragrafo 1, nella parte in cui sancisce che entro il 29 dicembre 2021, ciascuno Stato membro designa un ente (...) che agisce in qualità di centro nazionale di coordinamento (...).

Il Regolamento, con portata generale e direttamente applicabile in ciascuno Stato membro, è entrato in vigore lo scorso 28 giugno 2021 e, frattanto, con il Decreto-Legge n. 82 del 14 giugno 2021 recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale" (pubblicato nella GU Serie Generale n.140 del 14-06-2021) il Governo ha dato segnale di proattività, di fatto aggiornando l'architettura nazionale di sicurezza cibernetica, da ultimo definita con la Direttiva del Presidente del Consiglio dei ministri del 17 febbraio 2017, recante "indirizzi per la protezione cibernetica e la sicurezza informatica nazionali".

Vale la pena di evidenziare che già con la Legge 7 agosto 2012, n. 133 sono stati progressivamente attribuiti al Dipartimento delle informazioni per la sicurezza (DIS), compiti e funzioni pienamente rientranti nell'ambito della salvaguardia della sicurezza nazionale.

L'iter di conversione del Decreto-Legge è stato avviato con assegnazione alle Commissioni riunite I Affari Costituzionali e IX Trasporti in sede referente, in relazione all'Atto n. 3161 presentato il 14 giugno 2021, con parere delle Commissioni II Giustizia (ex articolo 73, comma 1-bis, del regolamento, per le disposizioni in materia di sanzioni), III Affari Esteri, IV Difesa, V Bilancio e Tesoro, VI Finanze, VII Cultura, X Attività produttive, XI Lavoro, XII Affari sociali, XIV Politiche UE, Commissione parlamentare per le questioni regionali e Comitato per la legislazione.

In estrema sintesi, l'impianto normativo disegnato dal nuovo decreto che si compone di 19 articoli provvede:

- a definire la Governance in materia di cybersicurezza;
- a razionalizzare le competenze in materia di cybersicurezza attualmente attribuite ad una pluralità di soggetti istituzionali;
- a supportare lo sviluppo di capacità industriali, tecnologiche e scientifiche nel campo della cybersicurezza, in un'ottica di autonomia strategica nazionale ed europea nel settore;
- a dare attuazione al Piano Nazionale di Ripresa e Resilienza (PNRR);
- a mettere in stretto raccordo l'architettura di cybersicurezza nazionale con il Sistema di informazione per la sicurezza della Repubblica previsto dalla legge 3 agosto 2007, n. 124, a fronte di una chiara separazione di competenze a tutela della sicurezza nazionale nel dominio cibernetico dell'attribuzione di poteri di controllo al Comitato parlamentare per la sicurezza della Repubblica (Copasir);
- a promuovere una gestione coordinata, con i diversi attori coinvolti, delle attività di prevenzione, preparazione e risposta a situazioni di crisi, anche mediante la costituzione, nell'ambito dell'istituenda Agenzia, del Nucleo per la cybersicurezza.

Ogni società è una società [fatta] di software

Nel mondo delle app l' azienda " È " la propria app.

di ***Paolo Da Ros***

Con software si intende quello strumento che una volta velocizzava le attività manuali e che poi passò a velocizzare i processi, fino ad arrivare ai giorni nostri in cui lo scopo è di velocizzare i processi aziendali.
D'altra parte le applicazioni definiscono la struttura interna di un'azienda e la modalità con cui questa si rapporta con il mondo esterno. Spesso però questo concetto non è chiaro: nella percezione del cliente la banca coincide ancora con l'app per il banking.
Una volta realizzata la connessione tra azienda e le funzionalità del suo software (il cosiddetto approccio digital), è sulle applicazioni che occorre lavorare per costruire posizioni di vantaggio competitivo. È fondamentale migliorare costantemente le funzionalità, con rapidità, e la sicurezza.

La velocità è indispensabile: se lancio un nuovo prodotto, ho comprato gli spazi pubblicitari e ho registrato gli spot, non posso permettermi che i commerciali non abbiano in tempo la app che serve per concludere la vendita.

Negli anni il miglioramento del ciclo di sviluppo è stato affidato alle metodologie. Structured programming, rapid prototyping, RAD, extreme programming, Agile sono solo alcune delle parole chiave.

In passato il contesto architetturale era stabile: su un mainframe, in ambiente client server o web, l'applicazione era sempre "di casa" e in più, con internet, la postazione dell'utente poteva essere esterna.
L'arrivo del Cloud Native Computing ha cambiato tutto. Il cloud non è più solo un modo semplificato, rapido ed economico per ottenere quello che prima richiedeva lunghi tempi di progettazione e approvvigionamento, ma abilita una nuova architettura applicativa.

In presenza di applicazioni monolitiche, i micro servizi, ognuno completamente indipendente e fornito del

necessario per il proprio funzionamento all'interno di un container, garantiscono flessibilità. Ogni container a sua volta può girare tramite qualsiasi fornitore di servizi CaaS (Container as a Service). I container vengono orchestrati da piattaforme che gestiscono i carichi di lavoro, il numero di istanze di un micro servizio e il cloud su cui tali istanze girano.

Una prima implicazione in termini di sicurezza è la "scomparsa del perimetro": non esiste più un'unica entità al cui interno girino le applicazioni, queste possono infatti trovarsi su qualunque fornitore CaaS.
Si parla quindi di Software Defined Perimeter: un perimetro "virtuale" con conseguenze sulla sicurezza, di cui in questa sede non andremo a parlare.

I micro servizi "containerizzati", completamente autonomi, consentono enormi guadagni di velocità di sviluppo. A rallentare il processo resta solo il Security Testing.

Se in passato si parlava di Dynamic Application Security Testing e di Static Application Security Testing, adesso si inizia a parlare di Interactive Application Security Testing.

In questo contesto però è da valutare anche un altro aspetto. Il PCI Council, ovvero l'Ente che supervisiona la sicurezza dei pagamenti con carta di credito, sta emettendo due nuovi standard: il Software Security Framework e il Secure Software Life Cycle (Secure SLC) Standard. Definiti per supportare la sicurezza dei pagamenti, i due nuovi standard riempiono uno spazio lasciato vuoto per troppo tempo.

Fino ad oggi le aziende che volevano mettere in sicurezza le proprie applicazioni avevano come unica proposta di mercato quella degli strumenti tecnologici. Con i nuovi standard si rendono disponibili delle best practices e delle linee guida che supportano l'aspetto organizzativo della messa in sicurezza delle applicazioni.

La privacy differenziale non è un mostro a tre teste

di ***Valentina Arena***

Viviamo in una società dipendente dalle informazioni, viviamo in quella che viene definita dai maggiori filosofi di questo tempo infosfera.

Un enorme quantità di dati processati, quotidianamente, dalle nuove tecnologie e dai social network che sempre di più condizionano la nostra esistenza.

Un mondo in cui si registra, si scrive e si memorizza tutto, ancor prima di valutare ciò che effettivamente serve ed è veramente importante; si condivide tanto senza conoscerne i rischi e valutarne le implicazioni e si cancella sempre meno.

Se questa sovrabbondanza di dati, per un verso, rappresenta un'opportunità straordinaria di miglioramento della società e delle relazioni tra le persone (rivoluzionando entrambe); per un altro, innesca implicazioni negative connesse alla messa in circolo di informazioni preziose e vantaggiose, pertanto, appetibili per altri soggetti.

In questo contesto, agli addetti ai lavori, è attribuito il compito di individuare i rimedi più adeguati per tutelare queste informazioni. Per quanto possa sembrare complicato, e non lo è, proverò a spiegare una tecnica piuttosto "recente" utilizzata, oggi, dai grandi colossi informatici. Per fare due nomi Google ed Apple in cui ogni giorno ci imbattiamo.

Il suo nome è privacy differenziale e no, non è un mostro a tre teste! È piuttosto una strana misura innovativa e funzionale alla protezione delle nostre informazioni.

Prima di rendervela comprensibile, perlomeno provarci, è imprescindibile aprire una piccola parentesi su due concetti: 1. anonimizzazione e 2. randomizzazione da cui, tra l'altro, tutto parte.
Partiamo con il primo.
Che significa rendere anonimo qualcosa o qualcuno?

Beh, non dobbiamo scomodare grandi matematici o studiosi della materia per comprendere che anonimizzare voglia dire nascondere l'identità di qualcuno alla quale, dunque, non si potrebbe più risalire.
Il secondo fa, invece, riferimento al concetto di casualità. Almeno una volta nella vita, a tutti, è capitato di affermare la presente frase: "ho scelto questo ristorante, così…. random".

Ebbene, tecnicamente, le due nozioni sono sorelle e vediamo perché.

Con l'anonimizzazione viene interrotta l'associazione diretta o indiretta con il soggetto cui quel dato si riferisce.

La randomizzazione, dal canto suo, produce lo stesso risultato introducendo però una cosa in più per giungere all'obiettivo: l'elemento di causalità, cioè il fattore random (definito rumore tecnicamente).

Questa doverosa premessa mi consente di accendere i riflettori su una circostanza. Sebbene si nasconda l'informazione di partenza, purtroppo, non possiamo decretare con una percentuale di certezza del 100% che proprio quel dato, nascosto, trapeli.

Si è assistito infatti piuttosto recentemente a casi di ri-associazione a causa di una sempre maggiore diffusione delle nostre informazioni sul web e che consentono agli informatici smanettoni di risalire alle informazioni complete.

Una tecnica che garantisce rispetto alle altre una maggiore difficoltà di re-identificazione al soggetto cui il dato si riferisce è appunto la privacy differenziale che appartiene alla famiglia della randomizzazione (quella che applica il fattore random/causalità) e che per funzionare bene necessita di una quantità di dati piuttosto importante.

Il procedimento che segue è a grandi linee il seguente:
Poniamo che, ad un campione di persone, venga fatta una domanda, per la quale sono ammesse solo due risposte "si" oppure "no".
Prima di raccogliere la risposta, si inserisce del "rumore" cioè altre informazioni random (a caso) che materialmente sporcano il dato nascondendo l'identità di chi ha generato le informazioni.

Come vengono inserite queste informazioni ulteriori e a caso?

Lanciando metaforicamente una monetina.
Se viene "testa" verrà registrata la vera risposta.
Se viene "croce", si rilancia una seconda; se viene "testa" allora si registra "si", se viene "croce" si raccoglie la risposta inversa cioè "no".

Il "lancio della monetina" è l'esatta esplicazione del concetto di random il quale, attraverso il principio di casualità consente di oscurare i dati reali e, quindi, di non identificare il soggetto cui appartengono.

Per concludere l'analisi sul tema mi piaceva fornirvi un esempio di applicazione pratica nel quale, magari, ci siamo imbattuti in diverse occasioni ma non ne abbiamo mai compreso il funzionamento.

Ebbene, svelato l'arcano.

Si chiama RAPPOR (Randomized Aggregatable Privacy-Preserving Ordinal Response) ed è un tool integrato in Chrome utilizzato per analizzare e realizzare grafici di dati. Se sulla barra di ricerca digitate il nome del vostro locale preferito, qualora avesse deciso di implementarlo, potreste rendervi conto dei giorni e delle ore in cui presso quell'esercizio risulta esserci più afflusso. Incrociando i dati che ogni giorno mettiamo in pasto alla rete RAPPOR anonimizza i dati degli utenti prima di analizzarli, consentendo agli sviluppatori di Chrome di leggerli senza poter risalire alle abitudini o ai comportamenti del singolo utente.

Dati e considerazioni dall'indagine OAD 2020 sulla cybersecurity in Italia durante la fase iniziale della pandemia di Covid-19

di ***Marco R. A. Bozzetti***

L'Osservatorio Attacchi Digitali in Italia, indicato con OAD, è l'unica indagine online indipendente ed autorevole in Italia sugli attacchi digitali intenzionali ai sistemi informativi di aziende e Pubbliche Amministrazioni (PA), Centrali e Locali, operanti in Italia. OAD è un'iniziativa ideata e realizzata annualmente dal 2008 da Marco Bozzetti con la sua società Malabo Srl[1] , insieme ad AIPSI[2] , capitolo italiano della mondiale ISSA, a uno o più Media Partner[3] e con l'importante collaborazione della Polizia Postale e delle Telecomunicazioni che fornisce annualmente significativi dati sugli attacchi alle infrastrutture critiche italiane, sulle frodi finanziarie e sul cyber terrorismo.

Il sondaggio OAD non prevede un insieme predefinito di rispondenti, ma consente ai potenziali interessati, in maniera rigorosamente anonima e libera, di compilare il questionario online le cui domande sono prevalentemente suddivise tra gli attacchi digitali subiti e le misure tecniche e organizzative di sicurezza digitale in essere. I potenziali rispondenti sono informati via email, newsletter, via web sia di AIPSI sia dei Patrocinatori dell'iniziativa. I rispondenti appartengono ad aziende di diversi settori merceologici e di diverse dimensioni (come numero di dipendenti), oltre che alla PA.
Questo approccio consente di rilevare un quadro specifico degli attacchi digitali in Italia, oltre che delle misure in essere per contrastarli.
Quadro che viene pubblicato annualmente in un rapporto finale, che è alla base di vari eventi tenuti da AIPSI anche con alcuni Patrocinatori. Tutti i rapporti finali OAD e gran parte della documentazione presentata nei diversi eventi, oltre ad articoli della stampa, sono raccolti e gratuitamente accessibili da uno specifico sito web curato da Malabo, https://www.oadweb.it/it/, che costituisce un vero e proprio "repository" di OAD.

OAD 2020 e Covid 19

L'indagine ed il conseguente Rapporto 2020 [4] coprono l'intero anno 2019 ed il primo quadrimestre del 2020, quando in Italia si è scatenata la pandemia Covid-19. Confrontando i dati tra i due periodi temporali, forniti dal medesimo bacino di rispondenti e quindi con piena validità statistica, è possibile avere un'idea di quanto il Covid-19 ai suoi inizi abbia impattato sugli attacchi digitali in Italia.
Questa pandemia, a livello mondiale e non solo italiano, ha scatenato una vasta gamma di attacchi digitali, causati principalmente dall'improvvisato – e spesso non sicuro - passaggio di molti al lavoro on line da casa e dal forte utilizzo di servizi via Internet, soprattutto per e-banking ed e-commerce, causato dal blocco della mobilità (lock down). Ma la realtà italiana delle imprese private e pubbliche differisce in modo sostanziale da quella degli altri paesi europei ed occidentali: siamo un paese ed un'economia basata sulle nano organizzazioni, come numero di dipendenti.

Facendo riferimento ai più recenti dati l'Istat[5] , in Italia il 99,91% delle imprese sono PMI, Piccole Medie Imprese, con meno di 250 dipendenti, e il 95% delle imprese ha meno di 10 dipendenti. Per le PA la situazione è analoga, anche se si hanno dati meno precisi e più datati: poche le PA di grandi dimensioni, come i Ministeri ed i grandi Comuni, moltissime le piccole e piccolissime organizzazioni tipicamente tra le PA Locali.

Il bacino di rispondenti emerso con OAD 2020 non solo copre quasi tutti i settori merceologici e le PA[6] , anche se la maggior parte delle aziende degli intervistati appartiene al settore ICT (30,8%), ma è ben bilanciato per le dimensioni delle organizzazioni. Infatti il 57,5% dei rispondenti appartiene a PMI, ed il 22,1 % appartiene ad organizzazioni con meno di 10 dipendenti. Organizzazioni piccolissime che sono la stragrande maggioranza in Italia, e che normalmente non sono considerate nelle indagini nazionali ed internazionali sulla cyber security.

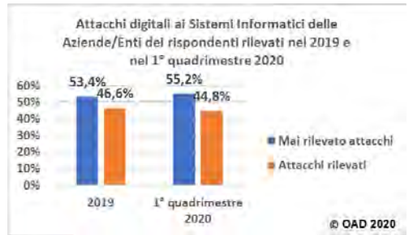


Fig. 1

La fig. 1 mostra la percentuale di attacchi digitali rilevati dai rispondenti nell'intero 2019 e nel 1° quadrimestre del 2020: 46,6% e 44,8% rispettivamente.
Queste percentuali potranno sembrare basse a molti lettori, tenendo conto delle numerose notizie sugli attacchi digitali.

Occorre però considerare due importanti fattori. Il primo è che il 30% circa dei rispondenti appartiene al settore ICT, e pertanto i propri sistemi informatici hanno mediamente un buon livello di misure di sicurezza, sia tecniche che organizzative, anche se talvolta il ciabattino ha le scarpe rotte .. Il secondo fattore, a mio giudizio ben più determinante, è che, in generale, i criminali informatici non sprecano tempo e risorse per attaccare le piccole organizzazioni, dove possono ottenere solo un profitto marginale e correre comunque il rischio di essere individuati dalla polizia. Gli aggressori prendono di mira per lo più le aziende più grandi, perché in quel caso il

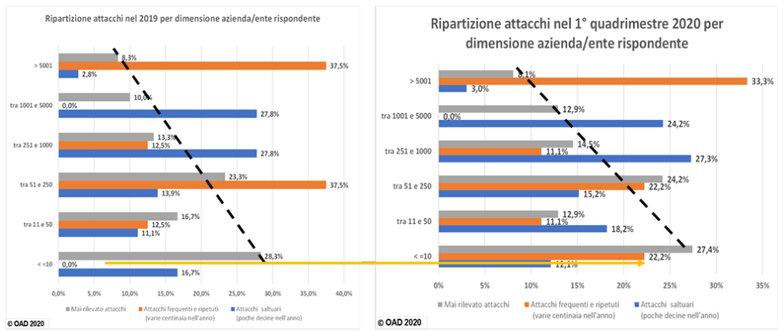


Fig. 2

1 Società di consulenza direzionale sull'ICT operante dal 2001: https://www.malaboadvisoring.it/it
2 AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, https://www.aipsi.org/ è il capitolo italiano della mondiale ISSA, https://www.issa.org/. Sono organizzazioni no-profit di professionisti ed esperti praticanti in ambito sicurezza digitale. L'obiettivo principale è la crescita professionale dei Soci, grazie a servizi che consentano l'aggiornamento continuo, la mentorship professionale, il supporto alle certificazioni individuali, lo stabilirsi di contatti a livello nazionale ed internazionale.
3 Per le ultime 3 edizioni di OAD il Media Partner è Reportec Srl: https://www.reportec.it/
4 Il Rapporto 2020 OAD completo è di 186 pagine A4, con 148 immagini e grafici, 11 Capitoli (147 pagine A4) e 9 Allegati (39 pagine A4). Nel Capitolo 11 i dati dalla Polizia Postale e delle Telecomunicazioni. L'intero rapporto completo ed una sua sintesi sono gratuitamente scaricabili da https://www.oadweb.it/it/rapporti-e-relativi-convegni/oad-2020/per-scaricaricare-la-sintesi-del-rapporto-2020-oad.html dopo aver fatto il login. La registrazione al sito è gratuita e richiede pochissime informazioni
5 ISTAT, Imprese e persone impiegate, set di DICA_ASIAUE1P, 2021. http://dati.istat.it/Index.aspx? DataSetCode=DICA_ASIAUE1P&Lang=it
6 La prossima edizione di OAD, la 2021, è denominata "Extended" in quanto si cerca di ampliare significativamente il numero di rispondenti nei diversi settori merceologici, oltre che nelle PAC e PAL, grazie soprattutto alla collaborazione con le associazioni operanti nei diversi settori. Per approfondire OAD Extended 2021, che a breve pubblicherà due questionari on line (uno di maggior dettaglio, l'altro più breve e semplice) si veda https://www.oadweb.it/it/oad-extended-2021.html.

guadagno illegale è ben più allettante: si consideri che ormai la principale motivazione di un attacco digitale è economica.

Questo è ben confermato dalla fig. 2: le due linee tratteggiate in nero, sia nel grafico per il 2019 che per quello del 1° quadrimestre 2020, mostrano come la % di non attacchi rilevati si riduce al crescere delle dimensioni dell'organizzazione attaccata. Il confronto tra i due periodi considerati mantiene la stessa tendenza logica nonostante l'esplodere della pandemia.

Financial Cyber Crime	1 gen - 30 apr 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Transazioni Fraudolente Bloccate	€ 20.200.000,00	€ 21.333.990,00	€ 38.400.000,00	€ 20.839.576,00	€ 16.050.812,50
Somme Recuperate	€ 8.700.000,00	€ 18.000.000,00	€ 9.000.000,00	€ 862.000,00	nd
Arrestati	nd	nd	nd	25	25
Denunciati	nd	nd	nd	2.851	3.772
Recupero/frode	43,06%	84,37%	23,44%	4,14%	

Fig. 3

L'unica differenza significativa è per i frequenti attacchi rilevati nelle piccolissime organizzazioni, fino a 10 dipendenti: lo 0% nel 2019 cresce fino al 22,2% (si veda la freccia arancione in fig. 2). Un aumento così forte deriva ovviamente dall'ampio utilizzo dei servizi di e-baking ed e-commerce, spesso attuato da questi soggetti senza le idonee misure di sicurezza, cui seguono specifici attacchi cyber, talvolta banali. L'impatto della pandemia sulla cybersecurity in Italia è inoltre ben evidenziato da alcuni dati della Polizia Postale e delle Comunicazioni riportati nella fig. 3; essa mostra la situazione della criminalità informatica finanziaria nei due periodi.

Come evidenziato dall'ovale rosso nella figura, le transazioni fraudolente bloccate nel 2019 sono dello stesso ordine di quelle dei soli primi 4 mesi del 2020. La crescita di questi attacchi e le ingenti somme di denaro coinvolte sono attribuibili all'uso intensivo dei servizi online durante i blocchi di mobilità imposti dalla pandemia di Covid-19.

Cosa è successo nel resto dell'anno 2020? Lo scopriremo con l'indagine del 2021, già iniziata e con i riferimenti nella nota n. 6. Ma fin d'ora mi auguro che tutti i lettori di questo articolo, e più in generale tutti gli iscritti ad Assintel, vogliano compilare uno dei due questionari previsti per OAD Extended 2021 e che saranno a breve accessibili dal sito www.oadweb.it.

Alcune considerazioni finali

Il Rapporto 2020 OAD fornisce molti dettagli sulle tipologie e sulle tecniche di attacco digitale rilevate, sulle possibili motivazioni e sugli impatti avuti, oltre che sulle misure di sicurezza tecnica ed organizzativa in essere nei sistemi informativi oggetto delle risposte selezionate. Tali dettagli, tecnici, organizzativi, legali e normativi, sono commentati dall'autore per aiutare il lettore a comprendere il fenomeno degli attacchi digitali nella realtà italiana, ed a come farvi fronte, verificando quali misure di prevenzione, di contrasto e di ripristino ha in atto rispetto a quelle che potrebbe o dovrebbe avere. Le misure di sicurezza organizzativa sono sovente carenti, soprattutto nelle piccole e piccolissime organizzazioni.
Come già evidenziato, l'Italia ha un numero grandissimo di queste organizzazioni, il che non la rende tra i paesi più attraenti ed allettanti per i criminali informatici che operano per lo più su larga scala e a livello mondiale.

La guerra informatica e gli attacchi di massa rappresentano un rischio crescente e grave anche per l'Italia e per le piccole organizzazioni, come è già accaduto in parte con la forte diffusione del ransomware, dovuta prevalentemente dalla mancanza o insufficienti misure di base di sicurezza informatica: in primis sistematici e completi back up e tempestivo aggiornamento dei software di base ed applicativi.

OAD 2020, rispetto alle edizioni precedenti, rileva un miglioramento e un rafforzamento delle misure di sicurezza digitale, sebbene i più moderni sistemi basati su tecniche di intelligenza artificiale siano ancora adottati in modo embrionale, e sono in prevalenza appannaggio delle imprese di grandi dimensioni.

La pandemia ha riportato prepotentemente in evidenza l'importanza e la necessità del digitale, e della sua effettiva sicurezza: e si sono evidenziate tutte le gravi carenze in Italia, anche infrastrutturali, da anni ben note. Ho personalmente qualche dubbio che l'effetto Covid-19 possa cambiare a breve questa situazione da tempo incancrenita. Il problema, a parte le dovute eccezioni, è soprattutto culturale, come anche fotografato dall'indicatore europeo DESI [7] sul livello di digitalizzazione dell'economia e della società per tutti i paesi dell'UE. L'Italia si posiziona nel 2020 al quart'ultimo posto complessivo, e all'ultimo in assoluto sul capitale umano.

Un'ultima considerazione rivolta al futuro. Le misure di difesa e le tecniche in uso inseguono l'evoluzione sempre più sofisticata e intelligente degli attacchi, ma sono quasi sempre in ritardo. L'elevata densità di vulnerabilità richiede approcci diversi e nuove logiche, rispetto alle attuali, con l'obiettivo di rendere tutti i sistemi ICT interconnessi a Internet intrinsecamente sicuri, per impostazione predefinita e per progettazione. La maggior parte dei sistemi informatici in Italia è ancora lontana da questo obiettivo.

La consapevolezza e le competenze in materia di sicurezza informatica devono essere aumentate a tutti i livelli al fine di migliorare in modo decisivo la lotta concreta contro i continui attacchi ed ai comportamenti degli utenti impropri quando non criminali. Solo un'efficace collaborazione tra le forze dell'ordine a livello mondiale, e soprattutto un uso reale e ampio dell'etica professionale sia di chi è coinvolto (lato offerta) che di chi decide (lato domanda) sulla cybersecurity può scoraggiare davvero la criminalità informatica, che non avrebbe più gli attuali ingenti ritorni economici.

7 https://digital-strategy.ec.europa.eu/en/policies/desi

Aggiornamento per SonicWall SonicOS

*Fonte: **https://csirt.gov.it/***

Sintesi

Gli aggiornamenti di sicurezza SonicWall sanano una vulnerabilità presente nel sistema operativo SonicOS.
Note: la vulnerabilità in oggetto è dovuta a una correzione incompleta della CVE-2020-5135, di cui si è data comunicazione precedentemente.

Rischio

Stima d'impatto delle vulnerabilità sulla comunità di riferimento: BASSO/VERDE (43,55/100)1.

Impatto

Internal sensitive data disclosure

Prodotti e versioni affette

SonicOS, versioni

- 6.5.4.7-83n
- 6.5.4.4-44v-21-955
- 6.5.1.12-3n
- 6.0.5.3-94o
- 7.0.0-R713 e precedenti
- 7.0.1-R1036 e precedenti
- 7.0.0.376 e precedenti

Azioni di mitigazione

In linea con le dichiarazioni del vendor, si consiglia di aggiornare i prodotti vulnerabili alle versioni più recenti disponibili.

Identificatori univoci vulnerabilità

CVE-2021-20019

Riferimenti

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0006

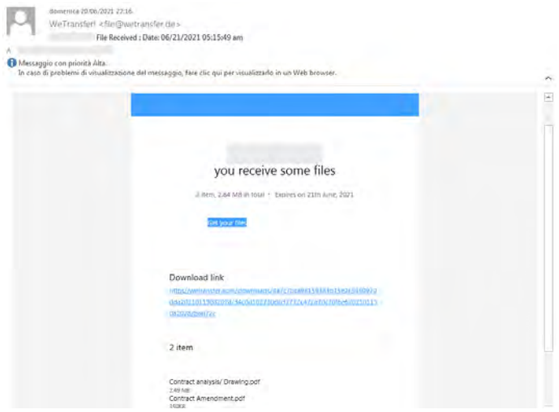
Campagna di phishing a tema WeTransfer

*Fonte: **https://csirt.gov.it/***

Descrizione e potenziali impatti

Recentemente è stata osservata una campagna malevola a tema "WeTransfer" mirata al furto di credenziali e password.

L'email (Figura 1) di phishing, scritta in inglese e apparentemente inviata da WeTransfer attraverso tecniche di spoofing, notifica alla vittima la ricezione di due file e contiene un collegamento ipertestuale e un link che puntano allo stesso URL (hXXps://gethukshop[.]com/jayredrict.html#<BASE64(destinatario_email)>&recovery=stopRecovery).



LA TRUFFA CORRE IN RETE: ATTENZIONE AI FALSI SITI DI TRADING ONLINE

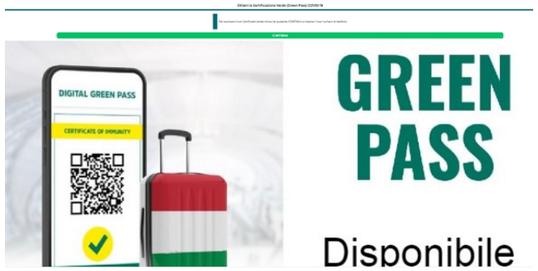
*Fonte: **https://www.commissariatodips.it/***

La truffa corre in rete: Personaggi famosi usati per falsi annunci pubblicitari su come guadagnare facilmente tanti soldi. False pagine web che sponsorizzano siti di trading online e che promettono guadagni milionari. Immagini contraffatte di giornali di informazione.
Foto di personaggi famosi, ignari della truffa, o di finti investitori internazionali che avrebbero ottenuto guadagni milionari. Questo è il meccanismo utilizzato da criminali informatici per ingannare le vittime e prosciugare i loro risparmi. La Polizia Postale invita i cittadini che volessero investire capitali con attività di trading online a rivolgersi solo a intermediari autorizzati, utilizzando solo strumenti di pagamento sicuri e tracciabili.
Verificare che il soggetto che propone il trading on line (ad es. su operazioni su forex) sia autorizzato, visitando i siti web della Consob e della Banca d'Italia;
Consultare la sezione "WARNING AND PUBLICATIONS FOR INVESTORS" dell'ESMA (la CONSOB europea) e verificare se, nei confronti del trader, altre autorità europee omologhe alla CONSOB, hanno pubblicato un avviso agli utenti (warning);
Verificare, attraverso i motori di ricerca sul web, la presenza di eventuali blog o forum sulla società di trading o del sito internet;
Diffidare di quei broker che offrono un rendimento fuori mercato (prospettando un ritorno economico in percentuali di elevata entità);
Fare trading con broker e su piattaforme conosciute e di provata affidabilità;
Non cadere nell'ulteriore trappola dei frodatori che, con il pretesto di sbloccare i rimborsi di quanto già "investito", richiedono il pagamento di ulteriori somme di danaro: si tratta di una vera e propria estorsione.

FALSO MESSAGGIO WhatsApp GREEN PASS

*Fonte: **https://www.commissariatodips.it/***

Negli ultimi giorni, numerosi utenti stanno segnalando la ricezione tramite whatsapp del seguente messaggio : " In questo link puoi scaricare il certificato verde Green Pass COVID-19 che ti permette liberamente di muoverti in tutta Italia senza mascherina".
Cliccando sul link, l'ignaro utente viene catapultato su una finta pagina istituzionale con numerosi loghi simili agli originali. Proseguendo nella navigazione sul sito, all'utente viene richiesto di inserire i propri dati personali e/o bancari con l'obiettivo di utilizzarli fraudolentemente.
La Polizia Postale raccomanda sempre di fare molta attenzione ai link indicati nei messaggi e di aprirli solo dopo averne accertato la veridicità della fonte di provenienza. Non inserire MAI i propri dati personali, soprattutto quelli bancari. Eventuali messaggi sospetti potranno essere segnalati sul portale della Polizia Postale www.commissariatodips.it



Anno 2 / Numero 4
2021

CYBER MAGAZINE

In questo numero:

Sanità nel mirino:
i cyber rischi e le possibili contromisure

L'incidente informatico:
come riconoscerlo e prevenirlo

Cinque buone abitudini per le aziende per minimizzare i rischi di ransomware

ASSINTEL CYBER SECURITY

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT