ASSINTEL CYBER SECURITY

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

ANNO 1
Aprile/Giugno
2020

CYBER Magazine

Lavoro da remoto e COVID-19

Come la Pandemia ha impattato la Cyber Security

Perché le aziende devono diventare Cyber-Resilienti

Indice

Paola
Generali

L’editoriale del Presidente Assintel

Nessuno di noi avrebbe mai immaginato di vivere uno scenario sociale ed economico così difficile, ma dobbiamo prenderne atto: COVID19 ci sta cambiando profondamente e nulla sarà più come prima, per questo tutti noi dobbiamo evolverci e riprogettare noi stessi e molte delle attività delle nostre aziende. Anche la Cybersecurity deve fare la stessa cosa, perché il nuovo contesto ha moltiplicato vulnerabilità e nuove minacce, legate ad un uso intensivo e diffuso della rete: Smart Working, Video Conferenze, didattica online e soprattutto socialità online portano con sé un forte – e non sempre evidente - bisogno di security. In questi giorni sulla bocca di tutti c’é la parola resilienza, che è diventata una parola chiave della nostra vita in questo momento, ma che nell’ambito della Cybersecurity è ordinaria, perché si trova nella sua stessa essenza.

Quando oggi qualcuno mi dice che la mia azienda è stata lungimirante a scrivere da sempre Business Continuity Plan che prevedessero anche lo scenario pandemico, io rispondo che non è lungimiranza ma una delle basi della Business Impact Analysis.

La differenza qual è allora?

Semplice, lo scenario pandemico ora si è verificato veramente.
Il Nostro Cyber Managazine vuole diventare un punto di riferimento autorevole per il mercato sia della domanda che dell’offerta in questo momento di evoluzione del contesto, che mette forzatamente la Cybersecurity tra gli argomenti di massima importanza.

Come la Pandemia ha impattato la Cyber Security

di ***Pierguido Iezzi,***

Non c'è dubbio che la pandemia si sia fatta sentire anche sul fronte Cyber Security. Ovviamente "remotizzare" milioni di lavoratori in un lasso di tempo molto breve non ha lasciato molto tempo a tantissime organizzazioni per mettere in piedi un perimetro di sicurezza informatica adeguato o che tenesse conto del nuovo scenario che si stava andando a creare. Questo è ovviamente comprensibile, laddove assicurarsi la business continuity diventa imperativo, soluzioni come lo Smart working diventano imprescindibili, proprio perché nascono per garantire la continuità del business attraverso la creazione di strumenti e processi che permettono ai tanti dipendenti, fornitori e clienti di poter collaborare da remoto.

Il rovescio della medaglia però è stato che si è creata in pochissimo tempo una superfice d'attacco per i Criminal Hacker nettamente più ampia.
Non dobbiamo dimenticare che lo Smart Working, dal punto di vista strettamente Cyber, porta 4 problematiche fondamentali: La dotazione aziendale standard è fuori dal nostro perimetro aziendale e quindi opera su reti di casa a volte non sufficientemente protette o, in moltissimi casi, deve interagire con dispositivi IoT non sicuri.
Come se non bastasse, alcuni lavoratori si saranno trovati costretti a lavorare sui propri device, sicuramente non allineati con le misure di sicurezza software installate – da best practice – sui device aziendali. Altra conseguenza dello Smart Working è stata l'impennata nell'utilizzo di connessioni VPN.

Queste permettono agli utenti di collegarsi alla rete aziendale direttamente dalla propria abitazione. Ma è stato dimostrato più e più volte come queste, specialmente nelle miriadi di edizioni free che esistono al momento, sono tutt'altro che una garanzia di sicurezza e affidabilità.

Se violate perché non sufficientemente sicure o non correttamente settate, potrebbero spalancare ai Criminal Hacker la porta per un attacco alla vostra azienda.

Come se non bastasse, nello smart working potrebbe presentarsi la necessità di utilizzare il controllo remoto, e nello specifico il Remote Desktop Protocol di Windows, per accedere ad una macchina o per procedure di help desk. Negli ultimi anni, sono stati osservati un numero crescente di cyber security incident in cui gli aggressori si sono collegati da remoto a un server Windows da Internet utilizzando RDP e si sono loggati come amministratore del computer.

La pandemia non ha fatto che accentuare la necessità di utilizzare il protocollo RDP, aumentando esponenzialmente quindi, il rischio che i Criminal Hacker riescano ad accedere alle macchine aziendali per compiere una serie di attacchi, principe tra tutti quello di installare ransomware. Per quanto riguarda altre tipologie di Cyber attacco che hanno visto l'aumentare dell'intensità non possiamo ignorare il Phishing. Questo per sua natura fa leva sui bisogni e le paure della gente, e cosa c'è di meglio per far abbassare

la guardia alle vittime delle email truffa a tema COVID-19? A partire dall'inizio del contagio sono state osservate numerose campagne di email dannose che sfruttavano l'esca del Covid-19 per cercare di convincere le potenziali vittime a fare clic. I criminali hanno inviato ondate di email che vanno da una dozzina a più di 200mila alla volta, e il numero di campagne tende ad aumentare. Circa il 70% delle email di phishing scoperte nelle ultime settimane sono utilizzate per consegnare malware e un ulteriore 30% mira a rubare le credenziali della vittima.

Ci sono stati anche attacchi ancora più diretti; l'esca, questa volta, sono state le mappe del contagio.

Si è trattato di diverse campagne per diffondere malware che miravano specificamente a colpire coloro che sono alla ricerca di presentazioni cartografiche della diffusione del virus su Internet, ingannandoli e convincendoli a scaricare ed eseguire un'applicazione dannosa. Questa, sul suo front-end, mostrava una mappa caricata da una fonte online legale, ma in background comprometteva il computer attraverso infostealer e malware di simile natura.
Il rischio in questo caso è trasversale, il mondo del Cyber Crime, anche durante la Pandemia opera su due concetti base: path of least resistance e vulnerability attacks.
Cosa significa?
Significa che i Criminal Hacker cercheranno nella maggior parte dei casi il percorso più semplice per attaccare le proprie vittime, senza badare troppo a chi stanno veramente andando a colpire. Questo va a braccetto con il concetto di vulnerability attacks; individuato un exploit, si cercano i sistemi che possono essere attaccati tramite la vulnerabilità prescelta dal Criminal Hacker. Poco importa che il bersaglio sia una PMI, una struttura sanitaria o una grande azienda strutturata.

Nel mondo del Cyber Crime as a Service il livello di skill richiesto è molto più basso di quanto si possa immaginare, attacchi preconfezionati vengono venduti a basso prezzo sul Dark Web già Ready to Use.

Questo concretamente significa che l'allerta deve essere generale perché l'aumento delle superfici d'attacco a disposizione non ha fatto altro che fornire più vittime potenziali ai Criminal Hacker.

È chiaro, perciò, che lo scenario descritto non fa che sottolineare ancora di più la necessità di consolidare e migliorare costantemente i fondamenti di ogni perimetro di Cyber sicurezza: il lato tecnologico e quello umano.
Da un lato infatti, è imprescindibile avere una chiara visione di quali possibili falle possono essere presenti in qualsiasi momento all'interno della nostra azienda. Effettuare regolari attività di Vulnerability Assessment e Penetration Testing garantisce la corretta individuazione di quelle problematiche non risolte che si potrebbero annidare all'interno del nostro perimetro per poi correggerle tempestivamente prima che i Criminal hacker siano in grado di sfruttarle.

Ovviamente, dobbiamo anche capire chi potrebbe essere interessato ad attaccarci. Qui entra in gioco la Domain Threat Intelligence, la conoscenza che permette di mitigare o prevenire questi attacchi. Fortemente basta sui dati, la Domain Threat Intelligence fornisce informazioni e indicatori utili per attuare migliori strategie di Cyber difesa e migliorare la resilienza del proprio perimetro aziendale.

Si tratta di una conoscenza basata su prove concrete, compreso il contesto, i meccanismi, gli indicatori, le implicazioni e i consigli su una minaccia esistente o emergente.

Queste informazioni possono essere utilizzate per meglio informare le decisioni riguardanti la risposta del soggetto preso di mira a tale minaccia o pericolo. In breve, la Domain Threat Intelligence è in grado di fornire una "actionable intelligence" tempestiva, contestualizzata e – soprattutto – facilmente interpretabile anche da chi non è espressamente del settore, ma è comunque in carica delle decisioni strategiche aziendali.

Sul lato "umano" della strategia di difesa l'attività deve essere duplice e attiva: servizi di Phishing concretamente ai propri smart worker come riconoscere ed evitare mail di phishing unita a formazione più tecnica e awareness, comunque amministrabili grazie a webinar e corsi online. Stesso discorso vale per chi ha scelto di utilizzare per la prima volta una VPN: bisogna sempre informarsi e scegliere con cura il prodotto più adatto alle nostre esigenze, non dimenticarsi mai di mettere in pratica le best practice di cyber security, effettuare una attenta e scrupolosa attività di security testing e adottare soluzioni di sicurezza proattiva.

Lavoro da remoto e COVID-19

di ***Riccardo Modena***

Premessa

Se possiamo trarre qualcosa di positivo dall'emergenza COVID-19 è sicuramente la consapevolezza che non siamo pronti.
Non lo siamo tutti e non lo siamo come vorremmo, soprattutto se pensiamo a quelle imprese italiane che, da un giorno con l'altro, si sono viste costrette a percorrere una marcia forzata verso l'applicazione del Lavoro da Remoto: una modalità operativa che si è fatta spazio nella vita di milioni di persone, con i suoi benefici, le sue difficolta ed i suoi rischi.

Lavoro da Remoto

L'introduzione del Lavoro da Remoto è un processo lento e complesso, che richiede lo svolgimento di diverse attività preparatorie: riorganizzazione dei processi, digitalizzazione delle attività, adozione di tecnologie abilitanti (es. piattaforme di collaborazione, Cloud, VOIP, ecc.) e di adeguati sistemi di sicurezza, istituzione di regole, formazione dei dipendenti, ecc.
Ma cosa succede quando le Aziende sono esposte ad un rischio concreto di interruzione del proprio Business che le costringe all'adozione quasi forzata del Lavoro da Remoto? Le priorità vengono rimescolate, la continuità del Business assume la prevalenza sul resto e in molti casi, la tutela delle informazioni e dei dati personali è messa in secondo piano.
Il Lavoro da Remoto offre infatti un'ampia serie di benefici alle Aziende che l'hanno sperimentato e lo applicano nel modo corretto. Tuttavia, la modifica delle abitudini lavorative e l'adozione di nuove tecnologie ampliano sensibilmente il "perimetro di sicurezza" dell'Azienda esponendo utenti, infrastrutture, applicazioni, informazioni e dati personali ai rischi del Cyber-Spazio. Rischi che non devono essere sottovalutati, tantomeno in un momento come questo: se l'obiettivo di ogni Cyber-Criminale è individuare nuove vulnerabilità e sfruttarle a proprio vantaggio, cosa c'è meglio di un'emergenza globale che ha improvvisamente costretto le Aziende ad introdurre nuovi strumenti operativi o estendere l'uso di quelli già adottati?
Per questo motivo l'applicazione del Lavoro da Remoto richiede controllo e preparazione, ma soprattutto la conoscenza dei rischi di Cyber-Security connessi a questa nuova modalità operativa e delle azioni necessarie per mitigarli.

Vulnerabilità e contromisure

Il Lavoro da Remoto presenta diversi rischi (es. difficolta di interazione, sovrapposizione di vita privata e vita lavorativa, solitudine derivante dall'abbandono delle consuetudini, ecc.). Tuttavia, per quanto ci riguarda, il podio è sicuramente ricoperto dai pericoli informatici, che trovano massima espressione negli attacchi di Cyber-Criminali a danno delle Aziende.

Tra i principali fattori di rischio ricordiamo l'utilizzo di dispositivi personali che spesso non assicurano il rispetto degli Standard di sicurezza definiti dall'Azienda, la vulnerabilità delle reti domestiche, l'utilizzo di connessioni non sicure per accedere ai sistemi aziendali, la difficoltà nell'addestrare i propri dipendenti e l'assenza di politiche per la sicurezza delle informazioni atte gestire le complessità del Lavoro da Remoto. I Cyber-Criminali possono sfruttare questi fattori di rischio e utilizzare diverse metodologie di attacco (es. malware, intrusione in reti non sicure, attacchi di ingegneria sociale, ecc.) per accedere in modo non autorizzato a dati e informazioni o impedire il corretto funzionamento dei servizi aziendali. Questi pericoli sono maggiori per le imprese di dimensioni minori, dove non è sempre presente personale con competenze specifiche nell'ambito della Cyber Security.

Misure minime di sicurezza

Quali sono, dunque, le misure di sicurezza che ogni Azienda deve adottare in questo particolare momento ed in generale quando s'intende affrontare la sfida del Lavoro da Remoto? La sicurezza di questa modalità operativa deve essere affrontata considerando tre dimensioni fondamentali: persone, processi, tecnologie.

Persone

Ciascun utente deve essere informato sulle modalità di svolgimento delle proprie attività al di fuori del contesto aziendale e sensibilizzato sui rischi a cui va incontro nel momento in cui utilizza lo strumento del Lavoro da Remoto. Soprattutto, deve essere reso consapevole del proprio ruolo come partecipante attivo nella

"catena" della sicurezza delle informazioni che, come insegnerebbe qualsiasi Cyber-Criminale, è tanto forte quanto il suo anello più debole.

Agire sulle persone significa prepararle ad affrontare una platea di minacce sempre più numerosa, fornendo loro gli strumenti necessari per proteggersi e le procedure da attivare in caso di emergenza (es. rilevazione di un incidente di sicurezza).
È anche importante analizzare le competenze interne e affidarsi a Partner competenti, in grado di supportare l'Azienda dal punto di vista operativo e di sicurezza.

Processi

L'attuale emergenza sottolinea l'importanza di definire piani e regole che permettano all'Azienda di garantire la continuità del Business e che orientino il comportamento degli utenti, al fine di mantenere gli Standard di sicurezza definiti anche nei momenti più critici. Per fare ciò occorre analizzare i processi interni, verificare se possono essere digitalizzati o resi più sicuri, formalizzarli e definire le regole che devono essere rispettate nello svolgimento degli stessi.

In mancanza del tempo necessario per svolgere queste attività, si suggerisce di predisporre un disciplinare rivolto agli utenti, usando come riferimento i principali Standard in tema di sicurezza delle informazioni (es. ISO 27001).

Tecnologie

L'ultima dimensione è la più complessa da gestire, perché richiede l'individuazione e l'adozione di tecnologie idonee a consentire il Lavoro da Remoto in sicurezza. Per fare ciò, occorre considerare i seguenti elementi "chiave":

- Sicurezza dei dispositivi: utilizzare preferibilmente dispositivi aziendali, configurati secondo gli Standard di sicurezza definiti dall'Azienda (es. antivirus, backup, aggiornamenti, ecc.);
- Autenticazione: i sistemi dell'Azienda devono poter essere acceduti solo dagli utenti autorizzati, verificandone l'identità degli stessi (es. autenticazione multifattoriale);
- Autorizzazione: utenze e privilegi devono consentire agli utenti di accedere solo ai sistemi, alle informazioni e ai dati personali necessari per lo svolgimento dell'attività lavorativa;
- Crittografia: la cifratura del disco fisso offre la garanzia che, in caso di furto del dispositivo, le informazioni e i dati personali non possano essere acceduti in modo non autorizzato;
- Sicurezza fisica: i dispositivi incustoditi devono essere dotati di automatismi per il blocco dello schermo in caso di inattività dell'utente, in modo da impedirne l'utilizzo da parte di soggetti terzi;
- Backup: i documenti devono essere sottoposti a Backup periodici per minimizzare il rischio di perdita di informazioni e dati personali in caso di malfunzionamento del dispositivo;
- Aggiornamento: l'aggiornamento costante del sistema operativo e del software di sicurezza assicura una protezione continua contro i pericoli del Cyber-Spazio (es. Virus, Malware, Trojan, ecc.);
- Sicurezza delle connessioni: la scarsa sicurezza delle reti domestiche può essere in parte mitigata attraverso l'utilizzo di connessioni crittografate (es. VPN, SSH, HTTPS, ecc.).

Un occhio alla Privacy

Le misure elencate devono essere progettate ed adottate in conformità con le norme vigenti in tema Privacy, analizzando gli impatti delle nuove modalità di lavoro sulla protezione dei dati personali e adottando adeguate contromisure.

Conclusioni

Di fronte all'emergenza COVID-19, molte Aziende si sono viste costrette a ricorrere al Lavoro da Remoto senza seguire l'approccio sopra descritto. Terminata la crisi occorrerà affrontare questa tematica in modo strutturato, cogliendo appieno i benefici che il Lavoro da Remoto offre all'Azienda e ai lavoratori.

Perché le aziende devono diventare Cyber-Resilienti

di ***Davide Giribaldi***

L'esperienza del Covid-19 è destinata a condizionare le nostre vite per diverso tempo e da un certo punto di vista cambierà in maniera irreversibile il nostro modo di essere imprenditori, ma fortunatamente ci lascerà l'opportunità di un cambiamento epocale trasformando la cybersecurity e la governance dei rischi nel nostro più importante fattore di successo post pandemia.

I motivi sono diversi e primo fra tutti un nuovo e diverso bisogno di fiducia.
Da alcuni anni le aziende di ogni settore economico e di qualsiasi dimensione, hanno intrapreso un processo di trasformazione digitale che l'emergenza Covid-19 ha improvvisamente accelerato, costringendoci a trasferire dentro le mura domestiche una parte delle infrastrutture aziendali con il risultato di averle indebolite e di avere creato un'immensa superficie di attacco per gli hacker che mai prima d'oggi si sono trovati davanti opportunità così ghiotte.

Lo stress derivante dalla forzata clausura, unito alla preoccupazione per qualcosa di improvviso e dal forte impatto sociale come questo nuovo ed inaspettato virus, hanno notevolmente abbassato le nostre difese; l'impossibilità di trasferire in così poco tempo "la sicurezza" aziendale dentro le nostre case ha fatto il resto, trasformando questo periodo in un incubo professionale per i responsabili delle infrastrutture IT.

Ma con tutte queste ingenerose premesse, cosa dovremmo aspettarci dal prossimo futuro?

Da questo punto di vista mi sento ottimista perché avremo la possibilità di migliorare i nostri servizi e di crearne nuovi, di studiare diversi modelli di business e cercare strategie più efficaci per rendere più competitive le nostre aziende e tutto ciò dipenderà dalla velocità e dalla profondità con cui sapremo adattarci ad un nuovo contesto.

Tutto ciò si chiama resilienza ed è lì che ci giocheremo una buona parte del nostro futuro imprenditoriale.
Se pensiamo all'evoluzione degli ultimi 24 mesi, uno degli aspetti più significativi della nostra trasformazione digitale è stato l'aumento esponenziale della quantità di dati e d'informazioni che abbiamo avuto a disposizione e che abbiamo dovuto gestire.

La loro diffusione è stata possibile grazie ad alcune tecnologie come il cloud e lo sarà ancora di più con la diffusione del 5G ed è avvenuta lungo alcune direttrici come il segmento mobile, l'IoT ed ovviamente l'intelligenza artificiale.
La conseguenza è stata un aumento considerevole delle superfici di attacco e quindi una maggiore vulnerabilità ed una più accentuata esposizione a pericoli, tanto è vero che negli ultimi 18 mesi si è registrato un considerevole aumento di attacchi sempre più complessi ed onerosi per le aziende che li hanno subiti.

E' quindi chiaro che la sfida per continuare ad offrire "fiducia" ai nostri clienti dipenderà in buona parte dalla nostra capacità ad individuare, gestire e mitigare i rischi cyber delle nostre infrastrutture in un ecosistema che si estenderà ben oltre il nostro perimetro ma che dovrà necessariamente coinvolgere anche i nostri fornitori, i nostri partner ed ovviamente i nostri clienti, in una sorta di collaborazione a 360 gradi in cui le sorti di ognuno di noi dipenderanno anche dalla capacità degli altri di fare squadra.
Raggiungere e mantenere la "cyber-resilience" implica la capacità di comprendere e gestire il rischio associato ad ogni singolo elemento dell'infrastruttura digitale attraverso il quale sono distribuiti i servizi e sono gestite le informazioni; per questo dovremo imparare sempre più ad individuare le priorità e rendere sicure le applicazioni i processi e le infrastrutture.
Cosa dovremo fare?

Dovremo elaborare ed integrare piani strategici di Governance, Risk, Compliance e Cybersecurity per comprendere l'impatto dei rischi sul business, per definire nuove policy ed adeguare i budget a nuove sfide che potranno essere vinte solo con l'allineamento dei rischi cyber alla mission ed alla vision aziendale.

Dovremo quindi allineare le strategie di business a quelle della cyber security, prendere coscienza di nuovi rischi, valutarne l'impatto e considerare ogni possibile danno a partire da quello reputazionale, distinguere le diverse priorità e trattarle adeguatamente, ma

soprattutto dovremo formare, istruire e mantenere costantemente preparati tutti i nostri collaboratori ad un modo più efficace di gestire l'azienda, che non potrà che svilupparsi solo attraverso una profonda consapevolezza dei rischi.

Come potremo farlo?

Anche se non credo esista una ricetta perfetta è probabile che un approccio per fasi sia la chiave di lettura ottimale per garantire la continuità operativa delle aziende anche in situazioni mutate come quelle post covid-19; prima di tutto dovremo valutare se il nostro modello di business sarà ancora applicabile o necessiterà di accorgimenti e di variazioni, successivamente dovremo valutare nuovi minacce ed opportunità, calcolare il loro possibile impatto sulle nostre aziende e valutare se e come trattare questi nuovi scenari di rischio.

Dovremo simulare gli incidenti, verificare i nostri piani di backup e soprattutto testare ogni possibile scenario in un contesto di miglioramento continuo e seguendo il più classico degli approcci al project management: plan, do, check, act!

Dovremo infine compiere lo sforzo più importante: cambiare le nostre abitudini imprenditoriali con coraggio ma con estrema fiducia nelle capacità dei nostri collaboratori dalle cui competenze dipende una buona parte della cyber resilienza aziendale.

Il covid lascerà certamente delle cicatrici, ma soprattutto immense possibilità di migliorare ciò che non ha funzionato, cambiare ciò che era sbagliato e creare ciò che non esisteva, in fondo anche questa è la mission degli imprenditori!

200 minacce informatiche distribuite sfruttando i nomi di note applicazioni di social meeting

di ***Kaspersky Lab***

A seguito della progressiva adozione di misure di distanziamento sociale, gli esperti di Kaspersky hanno esaminato il panorama delle minacce rivolte ad applicazioni di videoconferenza per assicurarsi che gli utenti siano protetti e che la loro esperienza d'uso di queste piattaforme di comunicazione sia positiva.

Le analisi condotte hanno rilevato circa 1.300 file con nomi simili ad applicazioni molto conosciute come Zoom, Webex e Slack. Le applicazioni di social meeting attualmente offrono alle persone un modo semplice per comunicare tramite video, audio o messaggi di testo in un frangente in cui non sono disponibili altri mezzi di comunicazione. Da questa situazione non hanno esitato a trarne vantaggio anche i criminali informatici, tentando di distribuire varie minacce informatiche sfruttando il nome di note applicazioni.

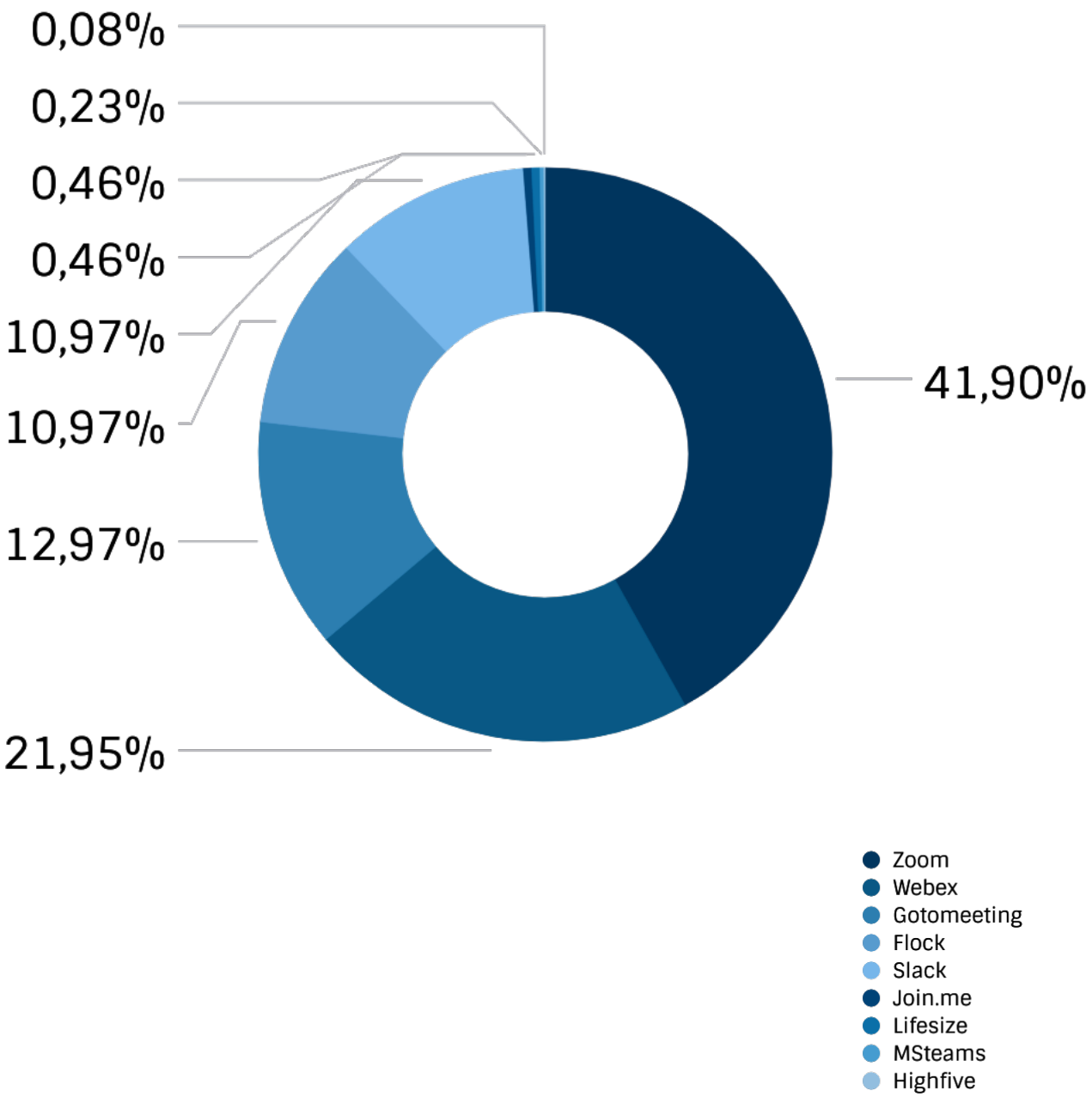
Dall'analisi di questi 1.300 file sono state rilevate 200 minacce. Le più diffuse sono quelle legate a due famiglie di adware, DealPly e DownloadSponsor.

Si tratta in entrambi i casi di installer che mostrano annunci o scaricano moduli adware. Questi software appaiono solitamente sui dispositivi degli utenti dopo essere stati scaricati da marketplace non ufficiali. Sebbene l'adware non sia un tipo di software dannoso, può comunque costituire un rischio per la privacy. I prodotti di Kaspersky rilevano e bloccano con successo DealPly e DownloadSponsor.

Oltre all'adware, in alcuni casi gli esperti di Kaspersky hanno individuato delle minacce nascoste sotto forma di file .lnk, ovvero abbreviazioni per applicazioni. In realtà la maggior parte di queste minacce è stata rilevata come Exploit.Win32.CVE-2010-2568, un codice malevolo abbastanza datato, ma ancora diffuso, che consente agli attaccanti di infettare alcuni computer con un ulteriore malware. Skype è l'applicazione di social meeting il cui nome è il più utilizzato dai criminali informatici per distribuire minacce informatiche. Gli esperti di Kaspersky hanno individuato120.000 diversi file sospetti che utilizzano il nome di questa applicazione. Inoltre, a differenza dei nomi di altre applicazioni, il nome Skype viene utilizzato per distribuire non solo adware, ma anche vari malware, in particolare Trojan.

"E' bene precisare che non è stato rilevato un picco drastico nel numero di attacchi o nel numero di file etichettati come note applicazioni di comunicazione. Il numero effettivo di file rilevati in-the-wild che stiamo osservando è piuttosto moderato. La situazione cambia quando, invece, si tratta di Skype, ma questo è riconducibile alla popolarità dell'applicazione, che, per molti anni, è sempre stata presa di mira dagli autori delle minacce informatiche. Nonostante ciò, riteniamo che sia importante far conoscere l'esistenza di tali minacce. Nello scenario attuale, in cui la maggior parte delle persone lavora da casa, è estremamente importante assicurarsi che ciò che viene utilizzato come strumento per i social meeting online venga scaricato da una fonte legittima, configurato correttamente e non presenti gravi vulnerabilità senza patch", ha dichiarato Denis Parinov, security expert di Kaspersky.

Share of files that spread under the guise of popular social meeting applications



Regione Toscana: falsa ordinanza del presidente della giunta regionale

Fonte: ***Commissariato di PS. Online***

Ancora una notizia falsa. Sta circolando una fake news della Regione Toscana, secondo la quale sarebbe stata revocata la possibilità di svolgere attività motoria nella regione per il contrasto e contenimento del covid19.

La Regione Toscana, che ha completamente smentito il documento, ha presentato una segnalazione di reato alla Polizia Postale di Firenze.

Si invitano gli utenti a verificare le notizie consultando esclusivamente il portale www.regione.toscana.it diffidando da messaggi o news che non siano direttamente riscontrabili rispetto alla fonte di provenienza.


REGIONE TOSCANA

Ordinanza del Presidente della Giunta Regionale N° 47 del 30 Aprile 2020

Oggetto:

Ulteriori misure per il contrasto ed il [illegible] della diffusione del virus COVID-19 in materia di attività mo[illegible] del 29 aprile 2020

Dipartimento Proponente: DIREZIONE [illegible] E PROTEZIONE CIVILE

Struttura Proponente: DIREZIONE [illegible] TEZIONE CIVILE

Pubblicita'/Pubblicazione: [illegible] (PBURT/BD)

FAKE NEWS

Sapete cos'è il Captcha?

Fonte: ***Commissariato di PS. Online***

Il Captcha è un acronimo che sta per "completely automated public Turing test to tell computers and humans apart", ovvero "un test completamente automatico (Turing Pubblico) per distinguere i computer dagli umani".

il Captcha è un box di lettere e numeri, spesso di difficile lettura, che ci viene chiesto di decifrare e riscrivere prima di concludere un'operazione online.
Il Captcha aiuta a rendere più sicuri i siti web e a limitare bot, spam e tentativi di accesso non autorizzato ai siti internet.

Nato per scopi di sicurezza, questo strumento è talvolta utilizzato anche dai cyber-criminali, interessati a "proteggere" le proprie pagine di phishing, con le quali compiere le ben note frodi informatiche su larga scala, da indagini "indesiderate" compiute attraverso sistemi di analisi automatizzate.

Occorre dunque prestare massima attenzione, comprendendo che l'utilizzo di un captcha non vuol dire, di per sé, che il sito che stiamo visualizzando sia attendibile o sicuro.

Campagna Malware Android con riferimenti a INPS e COVID-19 (BL02/200407/CSIRT-ITA)

Fonte: ***csirt.gov.it***

Descrizione

INPS ha comunicato in un tweet nella giornata di ieri della presenza di una campagna volta a diffondere un'applicazione Android malevola. La campagna si appoggia al dominio inps-informa.online, palesemente falso. La homepage contiene un link per il download di una fantomatica applicazione per richiedere un bonus in denaro, se installata l'applicazione è in grado di infettare il telefono. L'applicazione è diffusa anche tramite QR code che rimandano al link per il download.

Impatto potenziale

Il malware cerca di indurre l'utente ad installare un servizio di accessibilità con il quale è in grado di leggere il contenuto dello schermo, fungendo da keylogger, e di simulare eventi di input (tocchi) per la dismissione di finestre di warning e l'elevazione ad applicazione Device Admin.
Inoltre è in grado di :

- leggere gli SMS ed occultare gli SMS ricevuti per carpire i pin 2FA;
- mutare tutti i volumi del cellulare e bloccare lo schermo come forma di riscatto;
- esfiltrare informazioni come numero di telefono, operatore e modello di cellulare;
- disinstallare applicazioni;
- mostrare pagine di phishing all'apertura di determinate applicazioni (di home banking, IM e client e-mail);
- impedire la propria disinstallazione (chiudendo la finestra di sistema ogni volta che ci si prova).
- Soluzione

L'applicazione (per i payload osservati dal CERT-PA) non utilizza exploit per l'elevazione a root, per cui è di facile rimozione con strumenti tipo ADB.

Vulnerabilità ad alta criticità su Cisco Firepower Threat Defense e relativo software Adaptive Security Appliance (AL01/200511/CSIRT-ITA)

Fonte: ***csirt.gov.it***

Descrizione

Nelle giornate del 6 e 7 maggio 2020, Cisco ha rilasciato un aggiornamento che corregge diverse vulnerabilità considerate altamente critiche, individuate in alcuni prodotti dedicati alla sicurezza delle reti. In particolare, sono risultati vulnerabili il software Cisco Firepower Threat Defense (FTD), che fa parte della sua suite di prodotti per la sicurezza della rete e la gestione del traffico, e il relativo software Adaptive Security Appliance (ASA), il sistema operativo dedicato alla sicurezza delle reti aziendali.

Impatti potenziali

Le vulnerabilità, se efficacemente sfruttate, potrebbero consentire a un utente malintenzionato di provocare esaurimento della memoria, avere accesso, modificare, cancellare dati sensibili o informazioni riservate, aggirare i meccanismi di autenticazione o creare condizioni di Denial of Service (DoS) sul dispositivo interessato.

Soluzione

Si raccomanda di procedere all'aggiornamento dei prodotti interessati.

ASSINTEL CYBER SECURITY

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

ANNO 1
Aprile/Giugno
2020

CYBER Magazine