Cybercrime, Confindustria avverte: ‘Italia vulnerabile per il basso livello di e-skill’

Non solo Pil azzerato e recessione economica che fotografa una “Italia ferma”, il Centro Studi Di Confindustria lancia anche l’allarme sulla sicurezza informatica del nostro Paese.

Secondo quanto afferma il **Centro Studi di Confindustria** nel suo rapporto di primavera presentato questa mattina “*la minaccia cibernetica a livello globale è destinata a crescere, di pari passo con la progressiva digitalizzazione della società e l’evoluzione degli strumenti di attacco. E l’Italia è “particolarmente vulnerabile*”.

Lo studio ha quantificato che il costo degli attacchi cibernetici potrebbero mettere a rischio inoltre i benefici economici della digitalizzazione: nel 2030 potrebbero infatti arrivare a pesare per l’1,2% del Pil mondiale.

Secondo quanto afferma il Centro Studi di Confindustria,” *l’Italia, dato che si trova al 25/o posto su 28 in Europa per livello di competenze digitali, è per questo “particolarmente vulnerabile agli attacchi”*.

Nel corso del 2018 gli attacchi cibernetici si sono quintuplicati, colpendo a largo spettri diversi settori economici, con in testa quello dall’energia (11% del totale), seguito dai trasporti e da telecomunicazioni e finanza.

Inoltre secondo i recenti sondaggi il 39% degli italiani ha

subito un reato o conosciuto una vittima del cybercrime (in linea con la media globale).

Le preoccupazioni maggiori che provengono dai cittadini sono il furto d'identità (81%) e dall'hacking dei social media (80%).

Tra i crimini più temuti seguono poi le transazioni fraudolente bancarie o su carta di credito (71%), false chiamate, mail e sms (70%), il furto dell'account e gli acquisti online fraudolenti (68%).

https://www.key4biz.it/cybercrime-csc-avverte-italia-vulnerabile-a-causa-del-livello-basso-di-competenze-digitali/251472/

Norsk Hydro May Have Lost $40M in First Week After Cyberattack

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/O8Y5im41dlI/norsk-hydro-may-have-lost-40m-first-week-after-cyberattack

---

Facebook Blocks More Accounts

Over Influence Campaigns

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/CY_foBEWjKE/facebook-blocks-more-accounts-over-influence-campaigns

---

LockerGoga Ransomware Neutralized by Shortcut Files

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Ythm0zNcas0/lockergoga-ransomware-neutralized-shortcut-files

---

Major U.S. Chemical Firms Hit by Cyberattack

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/4nX-qTjx0nY/major-us-chemical-firms-hit-cyberattack

---

UK Police Federation Hit by Ransomware

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/RYcXjUL867U/uk-police-federation-hit-ransomware

---

Russian Hackers Target European Governments Ahead of Elections: FireEye

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/ELU6JiswHYE/russian-hackers-target-european-governments-ahead-elections-fireeye

---

Industry Reactions to Norsk Hydro Breach: Feedback Friday

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/R02xmv7WbjU/industry-reactions-norsk-hydro-breach-feedback-friday

La diffusione della cultura del rischio, come si comportano le imprese?

*La rubrica **AssetProtection**, ovvero Riflessioni su sicurezza e terrorismo, a cura di Anthony **Cecil Wright**, presidente Anssaif (Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria). Per consultare gli articoli precedenti **clicca qui**.*
Cattivi esempi.

Un professionista si chiedeva su un social, pochi giorni fa, come mai i servizi di una grande banca possano essere stati fermi per quasi 36 ore, per quale causa ed oltretutto perché non abbia fornito una comunicazione ai clienti.

Nessuno ha potuto operare né con lo smartphone, né con il PC su Internet, né andando in agenzia: anche i dipendenti non potevano operare sui conti.

Nessuna comunicazione ufficiale, tranne – dopo una decina di ore di blackout – un "cartello", a livello online e mobile, che avvisava che a breve (24 ore dopo!) il servizio sarebbe ripreso.

Sembra che ciò sia stato dovuto ad un problema causato da una società di sviluppo software che aveva in corso i test di una nuova procedura. La stessa fonte ha affermato che degli hacker abbiano trovato modo di entrare nei sistemi e fare dei non meglio precisati danni (copiati i dati?). Un'altra fonte interna ha accennato invece ad un serio problema di

trasmissione dati (blackout di 36 ore? Possibile?). Quindi, in conclusione, non sappiamo quale sia stata la reale causa.

Perché ho citato questo episodio? Per cogliere l'opportunità di scambiare alcune considerazioni con i lettori, proponendo i seguenti interrogativi:

1. L'assenza di comunicazione ai clienti e stakeholders e i lunghi tempi per il ripristino di almeno alcuni servizi essenziali, non sta ad indicare che i piani di *business continuity e crisi management* non hanno funzionato o sono oramai un ricordo dei bei tempi passati?
2. Quante aziende sono nelle stesse condizioni?
3. Qualora un malware o degli hacker avessero effettivamente approfittato di qualche "porta" aperta su un server, a causa della concentrazione del personale sui test della nuova applicazione trascurando la sicurezza, non vorrebbe dire che l'esperienza recente (un noto ospedale romano) e quella passata (anni fa nella stessa azienda), non insegnano nulla?
4. Si parla, giustamente, di diffondere una adeguata cultura dei rischi informatici, ma è possibile che vi siano delle grandi aziende che non rispettano le norme più elementari?
5. L'esperienza insegna che la fretta di mettere in produzione una applicazione (pur giustificata dalla guerra alla concorrenza), non accompagnata da adeguate misure preventive e di *contingency*, continua a mettere a rischio la sicurezza dei cittadini. Non solo in banca. Il caso recente della Boeing non è drammaticamente eclatante?
6. Altresì grave è che l'esperienza passata non abbia alcun valore. Perché il personale con molta esperienza non viene incentivato a trasferire le sue esperienze ai più giovani? Perché non si fa tesoro dell'esperienza?

Credo che sia necessario un momento di riflessione.

Mi farebbe piacere ricevere un vostro parere.

Anthony.wright@anssaif.it

https://www.key4biz.it/la-diffusione-della-cultura-del-rischio-come-si-comportano-le-imprese/250873/

Sicurezza, privacy e smartphone: 5 consigli per proteggersi

Parlare di privacy e di smartphone sembra quasi un ossimoro: è chiaro che per poter utilizzare tutte le funzionalità di un dispositivo avanzato dobbiamo rinunciare ad una parte di essa, dagli spostamenti che facciamo ogni giorno all'attività fisica, dai siti che ci piace consultare spesso ai social network. Questo, però, non significa che dobbiamo arrenderci ad essere spiati 24 ore su 24, in ogni momento del giorno e della notte: la **consapevolezza** di come funziona il nostro amato/odiato dispositivo è **il primo passo da fare per evitare di renderlo ancora più invasivo e, in certi casi, anche pericoloso**. Ecco, quindi, 5 consigli utili per proteggersi dalle minacce più diffuse e per vivere più serenamente, senza necessariamente installare antivirus, antispam e altri tool pesanti sul vostro dispositivo.

Spegnete Wifi, GPS, NFC e Bluetooth se non si utilizzano

Lo so, siamo pigri e addirittura alcuni sistemi operativi oggi decidono per noi quando attivare e disattivare tali

funzionalità. Tuttavia dobbiamo abituarci a farlo manualmente, perché in questo modo non solo risparmieremo batteria, ma ci difenderemo da alcuni rischi potenziali, come ad esempio:

- accessi indesiderati da Bluetooth e Wifi (ovviamente se state sfruttando hotspot sicuri e le reti delle vostre **offerte ADSL e fibra di casa**, nessun problema);
- allaccio a reti senza fili realizzate ad hoc per attaccare e/o per appropriarsi di dati personali in modo illecito;
- furto di denaro attraverso l'NFC (sempre più possibile con la maggior diffusione dei pagamenti contactless);
- localizzazione continua attraverso il GPS (che sia Google o un criminale informatico, **è davvero necessario far sapere a tutti dove siamo in qualsiasi istante della nostra esistenza?**).

Occhio ai social network

Per questo punto sarebbe necessario scrivere un trattato in merito: i social network vivono e guadagnano con la raccolta dati ed è l'utente stesso a fornirli, **più o meno volontariamente** (il recente caso di **Facebook sotto inchiesta penale per la cessione di dati ad altre aziende** dovrebbe fare riflettere). Se, però, non potete fare a meno di Facebook, Twitter, Instagram, etc…, cercate di utilizzarli in modo intelligente, **evitando di condividere informazioni e contenuti particolarmente personali e/o sensibili**.

Ricordate, inoltre, che pubblicare sui social network **non è mai privato**, pur impostando le opzioni privacy in modo restrittivo: **ogni amico o follower può potenzialmente condividere a loro volta i vostri post, le vostre foto e i**

vostri dati, sia sullo stesso social network che all’esterno, con screenshot e altri sistemi. Insomma, prima di scrivere o pubblicare qualcosa, fatevi prima la seguente domanda: ne vale davvero la pena?

Occhio alle app

Gli store di Apple e Google vengono controllati regolarmente eppure non mancano casi, anche eclatanti, di app spia e/o particolarmente affamate di dati personali presenti all’interno dei cataloghi ufficiali e scovate in ritardo: **pensate, quindi, cosa potrebbe nascondersi negli store alternativi**. Se da questo lato Apple ha una politica di chiusura abbastanza stringente sulle app esterne (anche se con qualche metodo è possibile aggirare i blocchi), Android è molto più esposto alle app più pericolose.

-

Evitate, quindi, di installare applicazioni sconosciute, provenienti da fonti a rischio, ma dubitate anche quelle app che vi richiedono troppi permessi “strani” al momento dell’installazione. Un esempio: se state installando un’applicazione per la navigazione stradale è chiaro che sarà necessario l’accesso al GPS per poterla utilizzare, ma se state scaricando un’app per gli sfondi del telefonino che vi richiede la localizzazione geografica, beh, passate ad altro.

Evitate di rispondere o richiamare

numeri esteri

Se fate un lavoro che implica anche le comunicazioni con l'estero, ovviamente saprete già con quali Paesi sarete in contatto. Tuttavia, se non avete alcun interesse al di fuori dei confini nazionali e vi ritrovate chiamate con prefissi stranieri, evitate di rispondere o di ricontattarli. Spesso, infatti, **potrebbero nascondersi vere e proprie truffe**, che potrebbero scalarvi denaro e aprire la strada ad altri tipi di attacchi. Tra i servizi truffa via telefono più diffusi ultimamente, quelli provenienti da Tunisia ed est europeo (molto frequenti i seguenti prefissi: **+216, +373 e +383**);

Evitate siti e banner dubbi

Se state navigando su Internet dal vostro smartphone e vi si aprono pagine con annunci di vincite (iPhone, viaggi, pc, etc…), inviti alla compilazione di test o sondaggi mai richiesti, **quasi certamente si tratta spam** o, ancora peggio, un metodo per attaccare il vostro dispositivo e, quindi, i vostri dati. **Evitateli come la peste** e, se sono particolarmente frequenti, utilizzate browser più sicuri e dotati di ad block.

Non cliccate sui link

Che vi arrivino sulla mail, su WhatsApp, su Facebook, su Skype, non ha importanza: prima di cliccare su qualsiasi indirizzo Internet, anche proveniente da una fonte sicura, **chiedete conferma che sia stata quella specifica fonte ad averlo inviato**. Se ciò non è possibile, analizzate attentamente il link che avete ricevuto: è un indirizzo attendibile? Ha un dominio verosimile? Ha senso che il vostro amico, collega o familiare ve lo abbia inviato?

Sembra quasi paranoico doversi preoccupare di controllare qualsiasi link che vi venga spedito, ma sappiate che spesso le

minacce peggiori si nascondono su questi innocenti indirizzi. Attraverso link “malevoli” i criminali informatici **possono sfruttare i bug e gli accessi dei sistemi operativi e violarne la sicurezza**, consentendo il furto dati, l’accesso ai file o addirittura prendere il comando a distanza del dispositivo stesso (ad esempio attivando la fotocamera, cancellando o creando dati sulla memoria, etc…). Riuscite ora a percepirne le devastanti potenzialità? Bene, probabilmente il controllo dei link prima di un click ora vi sembrerà meno esagerato.

Ecco, quindi, 5 consigli per proteggervi dalle minacce sul vostro smartphone: non sono certamente gli unici ma possiamo considerarli certamente tra i più importanti e utili. Perché **il primo antivirus e il primo sistema d’allarme per i nostri dispositivi – è importante tenerlo a mente e averne consapevolezza – siamo noi**.

https://www.key4biz.it/sicurezza-privacy-e-smartphone-5-consigli-per-proteggersi/250792/