ASSITECA
CONSULTATIVE BROKER

La Gestione della Sicurezza Informatica in azienda:

Analisi, Prevenzione e Mitigazione

Emanuele Capra
Senior Consultant – Assiteca Consulting

Salerno, 13 dicembre 2018

CHI SIAMO
I nostri numeri

L'unica realtà di servizi professionali creata per assistere le aziende nella **gestione integrata dei rischi d'impresa.**

- Nata nel **1982**, oggi è il **primo gruppo italiano nel mercato del brokeraggio assicurativo**.
- Dal luglio 2015 è **quotata alla Borsa Italiana** – Segmento AIM Italia.
- Attività: **analisi dei rischi, consulenza, intermediazione e gestione del portafoglio assicurativo**.

CERTIFICAZIONI

- Bilancio civilistico e consolidato certificato dal 1985.
- Certificazione di Qualità secondo la norma ISO 9001:2008 dal 1997
- Bilancio Sociale dall'anno fiscale 2002/2003.
- Codice Etico e Modello Organizzativo ai sensi del D.Lgs. 231/01 in vigore dal 2004.
- Rating di Legalità 2018 ★★

65 milioni di ricavi

20 sedi in Italia

100 rappresentanze nel mondo

577 dipendenti e collaboratori

3.975 aziende clienti

4.985 analisi di rischio effettuate

650 milioni di premi intermediati

IL CONSULTATIVE BROKER

Un approccio innovativo alla gestione dei rischi aziendali

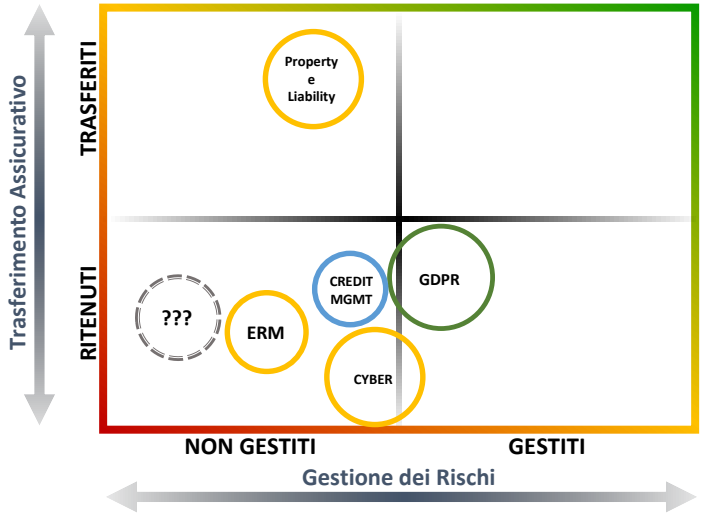
- **Approccio innovativo alla gestione dei rischi aziendali**: l'attività tradizionale di brokeraggio assicurativo è arricchita da specifici servizi di consulenza, per integrare l'offerta di soluzioni assicurative con strumenti interni di gestione dei rischi.
- La **metodologia di lavoro coniuga analisi, consulenza e intermediazione**, permettendo la costruzione di un efficiente ed efficace **sistema di controllo che previene, mitiga e protegge**.

APPROCCIO INTEGRATO

Risk management e risk transfer

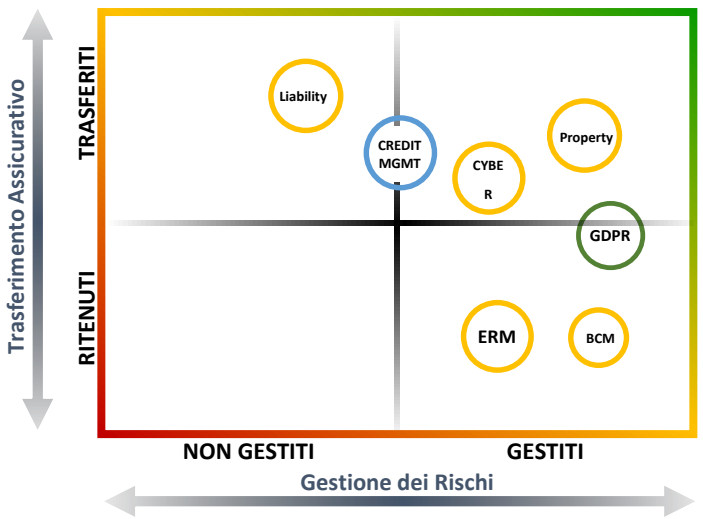
Si parte dalla mappatura dei rischi aziendali, identificando le principali aree critiche e le priorità di intervento, per poi disegnare la struttura ottimale di gestione dei rischi e affiancare il cliente nel percorso di mitigazione.

Mappatura attuale dei Rischi



- Parziale identificazione dei rischi
- Presenza di rischi ritenuti e non gestiti
- Elevato livello di impatto potenziale
- Costo non ottimale dei rischi trasferiti

Definizione struttura ottimale



- Mappatura dei rischi approfondita e continua
- Ottimizzazione dei rischi trasferiti e ritenuti
- Adeguato livello di rischio potenziale
- Ottimizzazione delle coperture assicurative

Rischi Strategici · Rischi Finanziari · Rischi Compliance · Rischi Operativi

ALTO — BASSO

Impatto economico

LO SCENARIO E' CAMBIATO !

Dalla guerra fredda a quella cyber

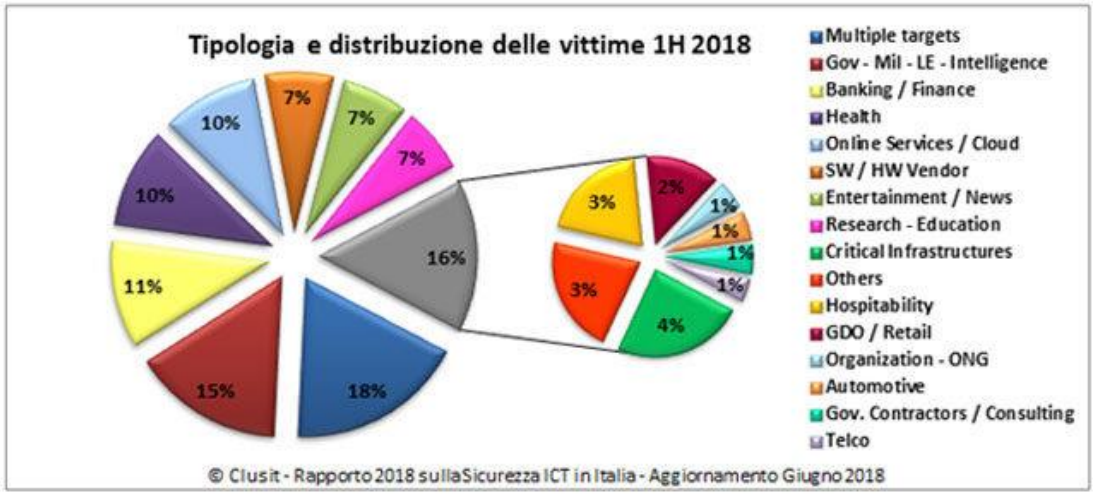
AZIENDE SOTTO ATTACCO

2018: il peggiore anno di sempre

Mail con iban ritoccato: truffe per oltre 1 mln ad aziende e utenti

(corbis)

L'inganno del 'Business email compromise' (B.e.c.) riguarda finora centinaia di utenti italiani dall'inizio del 2018, tra cui grandi imprese nostrane truffate per centinaia di migliaia di euro



Cybersicurezza, primo semestre del 2018 il peggiore di sempre

Nei primi sei mesi del 2018 il cybercrime è stato la causa dell'80% degli attacchi informatici a livello globale, risultando in crescita del 35% rispetto all'ultimo semestre 2017

Condividi 18

04 ottobre 2018

Una crescita dei cyber attacchi del 31% rispetto al semestre precedente, 730 attacchi gravi registrati e analizzati. Sono i dati della nuova edizione del Rapporto Clusit, presentata oggi al Security Summit di Verona. "Il 2018 si appresta a battere il triste primato dello scorso anno, definito l'anno del salto quantico della cyber-insicurezza. Il primo semestre è stato il peggiore di sempre", dicono gli esperti. Il picco maggiore a febbraio, con 139 attacchi: è il valore mensile in assoluto più alto negli ultimi 4 anni e mezzo.

» Facebook hackerato. Al via indagine federale. Warner: 'Congresso intervenga per proteggere privacy'

» Australia e Gb: "Servizi segreti russi dietro cyber attacchi"

Nei primi sei mesi del 2018 il cybercrime è stato la causa dell'80% degli attacchi informatici a livello globale, risultando in crescita del 35% rispetto all'ultimo semestre 2017.

Rispetto ai sei mesi precedenti considerati dal Rapporto, ad aumentare del 69% le attività riferibili al cyber spionaggio. E c'è una crescita a tre cifre nel settore Automotive (+200%); in ambito Research-Education (+128%); segue il settore Hospitability: hotel, ristoranti, residence hanno subito da gennaio a giugno 2018 il 69% di attacchi in più rispetto agli ultimi sei mesi dello scorso anno. In decisa crescita anche i crimini nei settori Sanità (+62%), Istituzioni (+52%), nei servizi Cloud (+52%) e nel settore della consulenza (+50%).

BANCHE

Nuove forme di criminalità

Puntoinformatico

IF 2018 5G IPHONE XS COPYRIGHT DAZN BITCOIN STREAMING LUCE E GAS Tutti gli speci

DarkVishnya: banche europee sotto attacco

Almeno otto banche dell'est Europa colpite da un attacco messo a segno dai cybercriminali attraverso l'installazione di un device fisico negli uffici.

Fonte: Kaspersky Lab
09/12/2018

Decine di milioni di dollari sottrati ad almeno otto **banche** dell'est Europa, attraverso attacchi che presentano modalità del tutto simili a quelle solitamente raccontate nelle pellicole hollywoodiane. È quanto emerso dalle indagini condotte da Kaspersky Lab e relative ad alcuni istituti del vecchio continente colpiti da **cybercriminali**.

del 08 Maggio 2017 — la Repubblica — QUOTIDIANO: ROMA — estratto da pag. 20

Il risparmio

Dopo anni di calo, nel 2016 un nuovo crollo: solo 360 casi, ma crescono le truffe informatiche

Rapine in banca in via d'estinzione anche per i ladri il bottino è digitale

ROSARIA AMATO

la grande distribuzione, pompe di benzina, locali. «Ma in ... ti spesi circa 600-700 milioni di eum tra misure di sicurez-

Unicredit ha subito due consistenti attacchi informatici, con sottrazione dei dati anagrafici di circa 400.000 clienti.

di
Alessandro Crea Tom's HardwareRedattore
26 Luglio 2017, 10:30
(Fonte UniCredit)

CONSULENTI

Deloitte: email al soldo dei cyber criminali

Un'altra grande azienda è finita nel mirino dei cyber-criminali. Questa volta il data breach riguarda la società di consulenza Deloitte, eletta solo qualche anno fa come migliore azienda in tema di cyber sicurezza

Roma - **Un attacco hacker ha aperto una breccia nei database di Deloitte**, azienda di consulenza e revisione, prima al mondo in termini di ricavi e numero di professionisti. L'attacco è venuto alla luce solo ora, nonostante sia perdurato per mesi a partire da ottobre/novembre 2016. Deloitte se ne sarebbe accorta solo a marzo avviando un'indagine interna. I cyber-criminali avrebbero ottenuto accesso privilegiato al server di posta, **intromettendosi nelle comunicazioni elettroniche tra l'azienda e i suoi clienti**. Favoriti dall'assenza di un sistema di autenticazione a due fattori, sono riusciti ad ottenere informazioni sensibili di numerosi clienti Deloitte, tra i quali spiccano grandi banche, multinazionali (anche farmaceutiche) e agenzie governative, come riportato da The Guardian.

CASELLE PEC

Violate 500mila caselle PEC di cui 98k della Pubblica Amministrazione

ASSITECA CONSULTATIVE BROKER

Rai News

ITALIA

ATTACCO HACKER DALL'ESTERO, VIOLATE 500MILA CASELLE PEC

Colpiti ministeri e Pa, con l'esfiltrazione di dati personali di magistrati e il conseguente blocco dei servizi delle Corti d'appello di tutta Italia. Dis: episodio allarmante, ora contromisure

19 novembre 2018 -

Un attacco "allarmante", "grave", che ha avuto "ricadute importanti". Il più significativo lanciato quest'anno contro l'Italia. Colpiti circa 3 mila soggetti tra pubblico e privato, oltre 30 mila domini e circa 500 mila pec, (la posta elettronica certificata), 98mila delle quali di appartenenti alla Pubblica amministrazione).

L'azione ostile ha mandato in tilt i tribunali, con l'esfiltrazione di dati personali delle Pec di magistrati ed il conseguente blocco dei servizi delle Cortid'appello di tutto il Paese, ma sono stati interessati anche i ministeri di Esteri, Interno, Difesa, Economia, Sviluppo economico. Ora, ha spiegato il vicedirettore del Dis (il Dipartimento delle informazioni per la sicurezza) con delega al cyber, Roberto Baldoni, la situazione è "sotto controllo", ma quanto accaduto dimostra che "vanno prese al più presto misure adeguate per innalzare le difese cyber".

Bersaglio degli hacker un fornitore dei servizi di Posta elettronica certificata Telecom di Pomezia

Il bersaglio degli hacker - sui quali indaga la Polizia postale - sarebbe stato un fornitore dei servizi di Posta elettronica certificata (Pec) Telecom di Pomezia (Roma). Il 12 l'azienda se ne è accorta e ha bloccato il servizio in via precauzionale. Il giorno dopo, l'incidente è stato notificato al Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche, che l'ha segnalato al Nucleo per la sicurezza cibernetica, istituito presso il Dis. Il 14 novembre, data la rilevanza dell'episodio, è stato informato il presidente del Consiglio, Giuseppe Conte, che ha convocato una riunione tecnica, svoltasi oggi al Dis, del Comitato interministeriale per la sicurezza della Repubblica (Cisr) per un approfondimento.

"Episodio allarmante, ora contromisure"

Al termine della riunione, fatto inconsueto per l'intelligence, Baldoni ha tenuto una conferenza stampa da un lato per rassicurare sulle operazioni di contenimento adottate: "La situazione è sotto controllo, il ripristino della funzionalità è tuttora in atto. Vanno cambiate le password di accesso alla Pec, ma questo devono farlo i

SEGRETI COMMERCIALI E KNOW HOW

Attacchi mirati a FinCantieri e Saipem - Spiate 900 aziende

L'industria navale in Italia è sotto una campagna di cyber attacchi mirati

Francesco Bussoletti

Dopo la scoperta di MartyMcfly, nasce la cyberforce tra Yoroi e il SOC di Fincantieri per analizzare le cyber minacce all'industria navale in Italia

R.it | Bologna

Preso l'Arsenio Lupin del web, spiava 900 aziende: frodata anche la Toyota

Laureato alla Sorbona, è riuscito a rubare 800 mila euro. Ogni anno 14 milioni di truffe informatiche alle aziende nella sola Emilia-Romagna

10 dicembre 2018

BOLOGNA - Una mail molto circostanziata, quindi assai credibile. Alla quale i manager di Toyota Italia, che ha sede a Bologna, hanno risposto con sollecitudine, provvedendo al pagamento di 249 mila euro, come prima tranche per un'operazione dal valore complessivo di un milioni di euro. La cattiva notizia è che si trattava di una truffa informatica, quella buona che gli stessi manager si sono accorti subito dell'inganno e con l'aiuto della polizia postale sono riusciti a bloccare l'invio di denaro. Di tentate frodi ai danni delle aziende, comprese quelle più strutturate, se ne registrano ogni giorno, anche in Emilia-Romagna e a Bologna. La polizia postale, nella sua attività di contrasto ai crimini informatici, sotto le due torri ha arrestato un 'pirata' del web che era riuscito a rubare ben 800 mila euro: sul tablet di questo bandito 4.0, laureato alla Sorbona, hanno scovato report su 900 società italiane, con i recapiti, gli account e dati di spesa di 6.500 tra presidenti e manager.

Eppure, quello dei reati informatici è "un fenomeno ancora molto sottovalutato dalle imprese", avverte il presidente di Confindustria Emilia, Alberto Vacchi, che oggi ha sottoscritto a nome dell'associazione un protocollo d'intesa con la polizia postale per la difesa del sistema delle imprese dagli attacchi telematici. La polizia delle telecomunicazioni tra il 2017 e il 2018 a Bologna ha registrato frodi informatiche per 14 milioni di euro ed è riuscita a recuperare circa 8,5 milioni di euro, comprese somme già trasferite su conti esteri. Non solo. Come ha spiegato Geo Ceccaroli, dirigente del compartimento di polizia postale dell'Emilia-Romagna, a fronte delle truffe scoperte sono stati avviati 88 procedimenti, con 25 denunce e un arresto (quello pirata con laurea nel prestigioso ateneo parigino).

Il nuovo contesto tecnologico "mette le imprese di fronte a problemi che non avevano mai affrontato. Il protocollo è importante per dare supporto alle imprese, ma anche per far toccare con mano il fenomeno, divenuto un problema da affrontare un maniera strutturale", avverte Vacchi. "Dopo 20 anni continuiamo a perdere. Continuiamo a investire in sicurezza, ma i crimini informatici aumentano. Bisogna cambiare approccio", suggerisce Michele Colajanni dell'Università di Modena e Reggio.

Innanzitutto, le aziende devono trovare il coraggio di denunciare. "Abbiamo sventato una frode che aveva superato le attività controllo", conferma Giorgio Polonio, manager di Toyota Italia. "Bisogna avere il coraggio di denunciare", sprona Roberto Sgalla, direttore centrale della polizia stradale, ferroviaria, delle comunicazioni e per i reparti speciali.

PROVIDER

QUORA – Facebook - WordPress: compromessi milioni di account

Attacco informatico a Quora: 100 milioni di account compromessi

Flash News Martedì, 04 Dicembre 2018 11:35

Il sito di domande e risposte Quora ha annunciato di avere subito un attacco informatico che ha interessato i dati di almeno 100 milioni di suoi utenti. Gli autori dell'attacco hanno potuto accedere a numerose informazioni, compresi indirizzi email e password, oltre a dati personali nel caso in cui un utente si fosse iscritto utilizzando un account di un social network già attivo.

Quora ha spiegato che alcuni dati erano già normalmente visibili sul sito, ma che l'attacco ha comunque esposto ulteriori informazioni e non sarà quindi sottovalutato. Ogni utente coinvolto riceverà nei prossimi giorni un'email con ulteriori dettagli e consigli per mettere in sicurezza il proprio account.

Fonte: Il Post

Facebook, nell'ultimo attacco colpiti 29 milioni di utenti. Di 400 mila copiato l'intero profilo

(ansa)

In un primo momento si pensava fossero stati interessati 50 milioni di utenti. L'attacco non ha riguardato Messenger, Instagram, Whatsapp. "I dati delle carte di credito sono al sicuro", garantisce Guy Rosen, vice presidente a capo della sicurezza della multinazionale. E aggiunge: "Stiamo collaborando con l'Fbi. Per ora non possiamo dire nulla sull'origine dell'attacco e sull'obbiettivo"

di JAIME D'ALESSANDRO

Cinquantamila siti WordPress infettati per minare criptovalute

Individuati 48.953 siti, dove un pezzo di codice permette agli hacker di insinuarsi negli smartphone e nei pc dei visitatori. L'obiettivo è "rapire" potere di calcolo dalle schede madri dei dispositivi e usarle per estrarre nuove criptovalute

FORNITORI

Attaccato il sito DELL
Rubati i dati dei passeggieri British Airways

Home » E-Gov & Privacy

Dell, sospetto attacco hacker

5 DICEMBRE 2018 COMMENTA

Dell ammette di avere subito un attacco hacker lo scorso novembre. Ecco tutti i dettagli ufficiali.

Attraverso una specifica nota pubblicata sul proprio sito **Dell** ha ammesso di aver subito un attacco hacker lo scorso 9 novembre. Al momento l'azienda ha già avviato le procedure per contrastare l'attività sospetta registrata sulla propria rete. L'attacco hacker, che sembra ormai confermato ha puntato ai dati sensibili degli utenti. Nello specifico gli hacker hanno manifestato il loro interesse nei confronti di indirizzi mail, nomi e password in hash. Al momento non sappiamo ancora se l'attacco hacker è riuscito a raggiungere il suo obiettivo. **Dell** ha voluto precisare che i dati relativi alle transazioni, come ad esempio quelli relativi alle credenziali delle carte di credito non sono stati intaccati.
L'azienda ha inoltre voluto precisare che al momento non esistono prove in grado di dimostrare la compromissione delle informazioni. Le parole usate all'interno del comunicato stampa ufficiale

British Airways: hacker rubano i dati di 380mila carte di credito

L'attacco, secondo la compagnia, sarebbe durato due settimane. Ora i "problemi" sarebbero stati risolti. In campo anche la National Crime Agency che si occupa dei casi più gravi e pericolosi

07 Settembre 2018

ROMA - British Airways ha subito un attacco hacker che ha trafugato i dati sensibili di 380mila carte di credito e degli stessi passeggeri che hanno prenotato un volo della compagnia tra il 21 agosto e il 5 settembre scorsi. L'attacco, rende noto il gruppo britannico, sarebbe durato due settimane.

"Sono stati colpiti i dettagli personali e finanziari dei nostri clienti che hanno effettuato delle prenotazioni sulla nostra app e sul sito. Abbiamo avvertito le autorità e in

ENTI PUBBLICI

Grandi città o piccoli comuni? non fa differenza !

LA STAMPA TECNOLOGIA

Virus informatico mette KO l'Ufficio tecnico del Comune di Arco

Gio, 27/07/2017 - 05:57

28 CONNECT | TWITTER | 0 LINKEDIN | EMAIL | STAMPA

PER APPROFONDIRE:
comune, arco, virus, computer

Tempo di lettura: ! minuto 36 secondi

Un attacco informatico o piuttosto un virus elettronico ha messo a dura prova nei giorni scorsi l'ufficio tecnico del municipio di Arco, in modo particolare il disservizio riguarda circa quattrocento pratiche edilizie che risultano danneggiate dal fenomeno. Adesso è necessario rimboccarsi le maniche e rimettere a posto tutto il materiale disastrato con ordine e una pazienza infinita.

Bloccati per 5 giorni i computer di 8.000 dipendenti pubblici della città di Atlanta

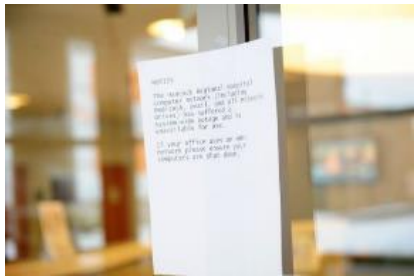
SamSam è un gruppo di hacker specializzato negli attacchi Ransomware: software malevoli che limitano l'accesso al dispositivo infettato. Di solito, per ripristinare l'accesso viene chiesto un riscatto in denaro. Alle autorità di Atlanta, SamSam ha chiesto 51mila dollari in bitcoin per far tornare a funzionare i sistemi informatici di molte delle istituzioni della città, che se si tiene conto dell'intera area metropolitana, conta una popolazione di quasi sei milioni di abitanti.
Durato cinque giorni e terminato giovedì 29 marzo, L'attacco ha colpito i sistemi informatici della corte di giustizia, dell'amministrazione comunale e dei centri per l'impiego. 8mila dipendenti pubblici non hanno potuto accendere i computer e per lavorare hanno dovuto utilizzare carta e penna. Fortunatamente, non è stato interessato il sistema per le chiamate al 911 o quello per il trattamento delle acque reflue. «Siamo sotto ostaggio», aveva dichiarato il sindaco Keisha Lance Bottom.

La città di Atlanta

SERVIZI ESSENZIALI

Hacker sequestrano i server di un ospedale americano e spengono una centrale elettrica

L'attacco ha paralizzato l'intera rete informatica.
Chiesto un riscatto in Bitcoin.



Le informazioni sanitarie conservate nei sistemi informatici degli ospedali non sono preziose soltanto per il personale medico: la loro natura di "dati sensibili" fa sì che siano anche ghiotte prede per gli hacker.

Lo scorso 11 gennaio si è avuta la dimostrazione di tutto ciò: in quel giorno l'Hancock Regional Hospital di Greenfield, Indiana (Usa) è rimasto vittima di un cyberattacco che ha compromesso l'intera rete informatica ospedaliera.
I computer si sono bloccati e hanno preso a mostrare soltanto una schermata che chiedeva il pagamento di un riscatto in Bitcoin: soltanto cedendo al ricatto - spiegavano gli autori dell'attacco - il personale dell'ospedale avrebbe potuto avere nuovamente accesso ai dati.
L'amministrazione ospedaliera non s'è però lasciata intimorire e ha deciso di spegnere ogni Pc, al fine di evitare il diffondersi di qualsiasi malware avesse colpito i computer, per poi contattare l'Fbi.
Le informazioni divulgate dagli investigatori sono a questo punto molto scarse, ma pare che l'attacco non sia stato facilitato da qualche tipo di errore umano, come un dipendente che abbocca a una email di phishing.
Attualmente la rete informatica dell'ospedale americano è tornata alla pieno operatività, ma l'Fbi non ha spiegato se il ritorno alla normalità sia stato ottenuto cedendo al ricatto oppure liberando il sistema dall'infezione. In ogni caso, l'amministratore della struttura ritiene che non ci sia stato alcun furto di dati.
Ciò di cui gli agenti federali statunitensi sono sicuri è che, a giudicare da quanto era sofisticato l'attacco, l'autore non era «un ragazzino quindicenne che vive nel seminterrato dei suoi».
In altre parole, non si è trattato soltanto di una ragazzata, ma dell'atto di un criminale con un obiettivo preciso.

Hackers shut down plant by targeting its safety system
It's the first known attack of its kind.

jon Fingas, 12.17.17
Hackers have already attacked critical infrastructure, but now they're launching campaigns that could have direct consequences. FireEye reported that a plant of an unmentioned nature and location (other firms believe it's in the Middle East) was forced to shut down after a hack targeted its industrial safety system -- it's the first known instance of a breach like this taking place. While the digital assault was clearly serious in and of itself, there are hints that it could have been much worse.

The malware, nicknamed Triton, hijacked a workstation using Schneider Electric's Triconex safety technology (typically used in power plants). The culprits hoped to modify controllers that could pinpoint safety problems, but some of those controllers entered a failsafe state in response and shut down the plant, leading operators to conduct the investigation that caught the hostile code. Triton was otherwise fairly sophisticated. It would try to recover failed controllers to avoid raising alerts, and would even overwrite its own programs with junk data if it couldn't salvage a controller inside of a given time window.
The hack wasn't made possible by a flaw in Triconex itself, FireEye noted. Instead, it appeared to be an "isolated incident."
While it's not certain who's responsible, FireEye said the hack was "consistent" with a "nation state" readying an attack. And that's concerning, especially if the perpetrators learn from their mistakes. While shutting down a power plant would be bad enough, it'd be worse if the malware could fool a safety system into allowing attacks that would damage the facility and lead to a long-term shutdown or an environmental disaster. In short, companies and governments alike may have no choice but to prioritize defending critical infrastructure if they want to avoid crippling attacks.

ALBERGHI
Catena Marriot:
rubati i dati personali di 500 milioni di clienti

Hackeraggio Marriot, parte la class action per il risarcimento

Davide Maniscalco

Gli hotel coinvolti nell'hackeraggio sono il W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels.

A rischio i dati personali di 500 milioni di clienti

03/12/2018 11:27 AM Temp Lettura articolo 4 min 0 Commenti

Oltre **12 miliardi di dollari di risarcimento per "danni e costi"** sostenuti per arginare le conseguenze del furto di dati. E' questa la cifra chiesta da un gruppo di clienti della catena alberghiera **Marriot a seguito dell'hackeraggio divulgato nei giorni scorsi. Stando a quanto scrive Ictbusiness.it** "un gruppo di clienti in Maryland e altri in Oregon **hanno fatto causa al colosso alberghiero"**. "La **class action** depositata in Oregon – si legge ancora sul sito – nasce per volontà di due viaggiatori d'affari, Chris Harris e David Johnson, che hanno chiesto 12,5 miliardi di dollari di risarcimento per "danni e costi" sostenuti per arginare le conseguenze del furto di dati. Ovvero 25 dollari a utente, il minimo da poter pretendere a fronte del tempo e del disturbo persi per bloccare la propria carta di credito".

A rischio le informazioni personali di circa 500 milioni di clienti

Nei giorni scorsi si è appresa la notizia che **dal 2014 sarebbe stato violato il sistema informatico della catena alberghiera Marriott**, con conseguenziale data leak di informazioni personali, anche sensibili. Secondo le dichiarazioni che si leggono in una nota del Marriott, a seguito di una segnalazione dell'8 settembre scorso e una successiva investigazione interna, **"soggetti non autorizzati hanno copiato e criptato delle informazioni effettuando azioni per ritirarle".** A rischio vi sarebbero le informazioni personali di circa 500 milioni di clienti. La catena alberghiera ha fatto sapere di avere già adottato tutte le **misure necessarie per "accelerare il rafforzamento della sicurezza dei terminali".** Le informazioni trafugate riguardano **nomi, indirizzi postali ed e-mail, numeri di telefono e del passaporto, data di nascita e altri dettagli normalmente indicati in fase di prenotazione**, tra i quali i più sensibili proprio il **numero di carta di credito e la data di scadenza**. Dunque, ancora una volta, la sicurezza delle informazioni personali viene esposta da vulnerabilità e rischi evidentemente non adeguate a garantire gli standards di protezione, con la conseguenza che **per ben 4 anni gli hackers, con fin troppa disinvoltura, hanno avuto accesso ai sistemi informativi aziendali della catena alberghiera.**

RISTORANTI

Bologna: hackerato l'home banking di Bruno Barbieri, Tutta colpa del wi-fi !

Arrestata una 33enne nigeriana. Aveva violato l'home banking dello chef e chiesto dei bonifici urgenti via e-mail

di MATTEO RADOGNA

Pubblicato il 20 luglio 2017
Ultimo aggiornamento: 19 luglio 2017 ore 23:06

Lo chef Bruno Barbieri

ANCHE LE STAMPANTI !

Hacker viola 50mila stampanti e stampa un messaggio

Hacker viola 50.000 stampanti per invitare tutti su un canale Youtube

L'attacco più strano della storia, ma anche il più innocuo.

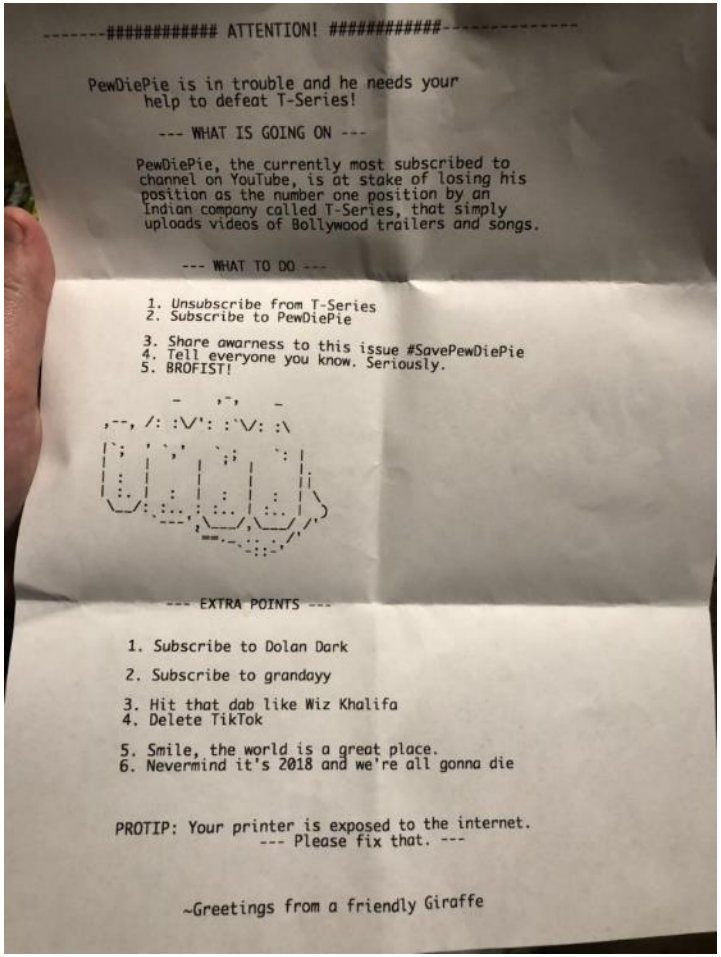
La possibilità di collegare la stampante alla rete locale (Wi-Fi o cablata) è così diffusa che ormai si trova anche sui modelli a minor costo.

Si tratta di una comodità che però ha un prezzo: se il firmware non è aggiornato, e la vecchia versione contiene una vulnerabilità, c'è la seria possibilità che questa possa venir sfruttata da remoto.

Ciò è esattamente quanto hanno scoperto - inizialmente più con perplessità che orrore, a dire il vero - i padroni di circa 50.000 stampanti in Stati Uniti, Canada e Regno Unito.

Trovando i suoi bersagli tramite Shodan, una sorta di motore di ricerca per i dispositivi vulnerabili connessi in Rete, l'hacker TheHackerGiraffe ha usato lo strumento noto come PRET (Printer Exploitation Toolkit) per creare uno script che ha costretto tutte quelle stampanti a stampare la medesima cosa.

Di che si trattava? Di un invito a iscriversi al canale YouTube di PewDiePie, discusso YouTuber che gode di una grande popolarità. Di qui, la perplessità dei possessori delle stampanti, che di punto in bianco hanno visto uscire dai loro apparecchi il testo che riportiamo in fondo all'articolo.



NON SEMPRE RIGUARDA GLI ALTRI 1/2

Scandalo Facebook: 214.000 italiani spiati

Mark Zuckerberg. Il Ceo di Facebook è atteso al Congresso Usa il prossimo 11 aprile

GDB ≡ Indice Leggi il GDB

Italia ed Estero

Home Lista articoli

Non si placa lo **scandalo Facebook-Cambridge Analytica** ma, anzi, iniziano a definirsi i contorni della vicenda. Gli utenti coinvolti nel mondo sono 87 milioni, a fronte dei 50 milioni stimati inizialmente, e fra questi ci sono poco più di **214mila italiani**. Da lunedì il social network inizierà ad avvisare le persone i cui dati sono stati condivisi dalla società. «La Commissione europea indagherà sul caso che consideriamo inaccettabile», ha riferito un portavoce dell'esecutivo. Mentre in Italia il Garante della Privacy intende raccogliere ulteriori elementi sugli utenti italiani.

«Dal 9 aprile diremo agli utenti se le loro informazioni sono state condivise da Cambridge Analytica», spiega Mike Schroepfer, Chief Technology Officer di Facebook. Le persone colpite dovrebbero ricevere un avviso che consentirà di vedere quali dei loro dati sono stati condivisi.

NON SEMPRE RIGUARDA GLI ALTRI 2/2

Anonymous pubblica gli account di 26.000 insegnanti italiani

Ansa
Internet&Social

Anonymous 'scippa' i dati di 26.000 insegnanti

Tweet postato da account LulzSecIta

- Redazione ANSA -
08 marzo 2018 - 17:07
- ANALISI

Suggerisci
Facebook
Twitter
Google+
Altri

Stampa

Scrivi alla redazione

Anonymous annuncia 'scippo' 26.000 dati di insegnanti © ANSA/ANSA

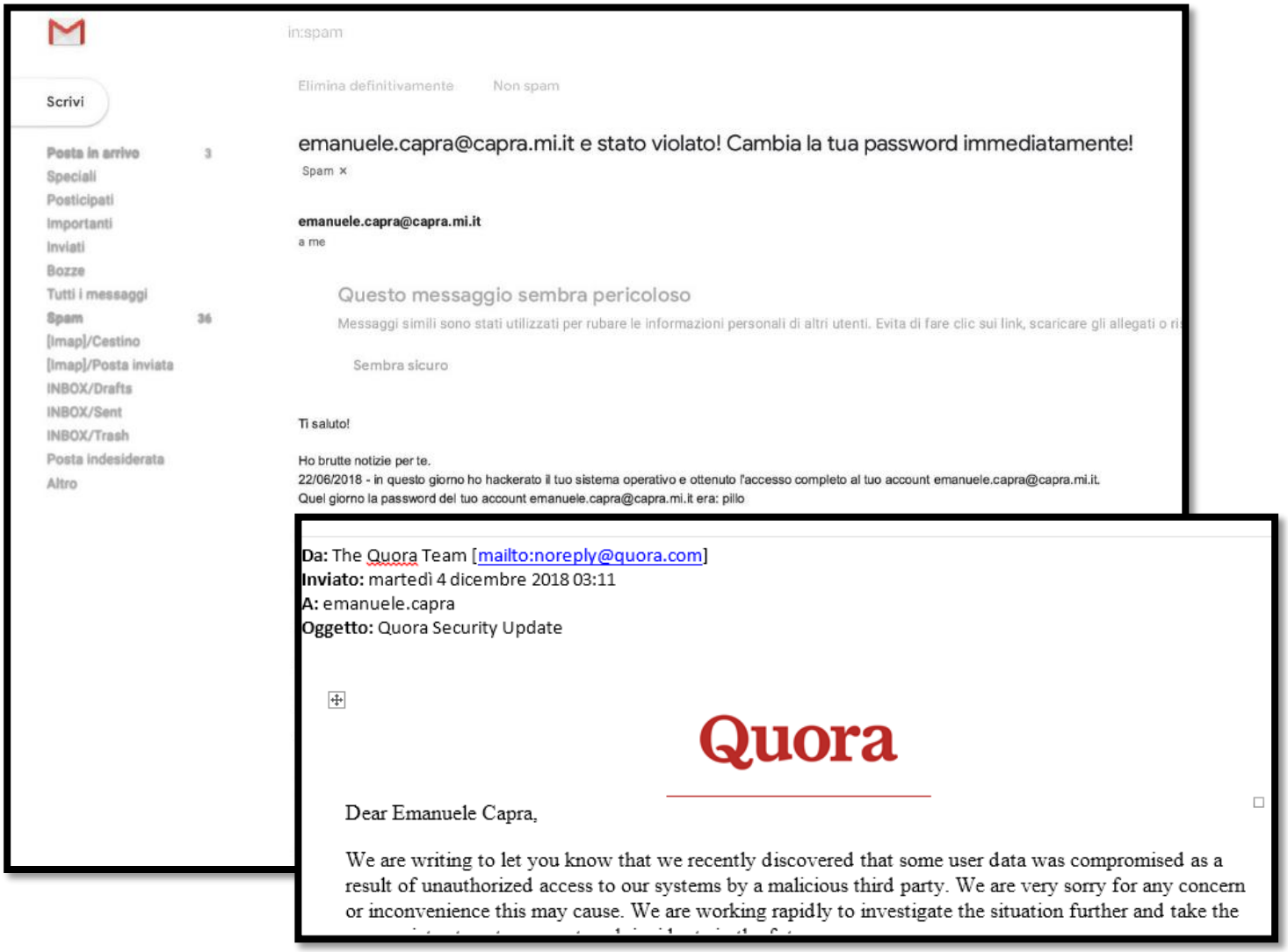
CLICCA PER INGRANDIRE +

ROMA - "Salve popolo, siamo qui oggi per comunicarvi con grande gioia, che circa 26.600 dati personali (email, password, cellulari, indirizzi) di maestre, insegnanti, referenti e dirigenti di molte scuole italiane sono entrate in nostro possesso!". E' il tweet postato, con data di ieri, dall'account LulzSecIta (uno degli account utilizzati dagli attivisti di Anonymous). Allegato un link in cui gli hacker, rivolgendosi direttamente alla ministra Valeria Fedeli, spiegano che l'obiettivo della loro azione è l'alternanza scuola-lavoro.

Con la combinazione giusta di email e password chiunque può modificare i voti sui registri elettronici!

NESSUNO E' ESENTE !

A me è successo 2 volte questa settimana…



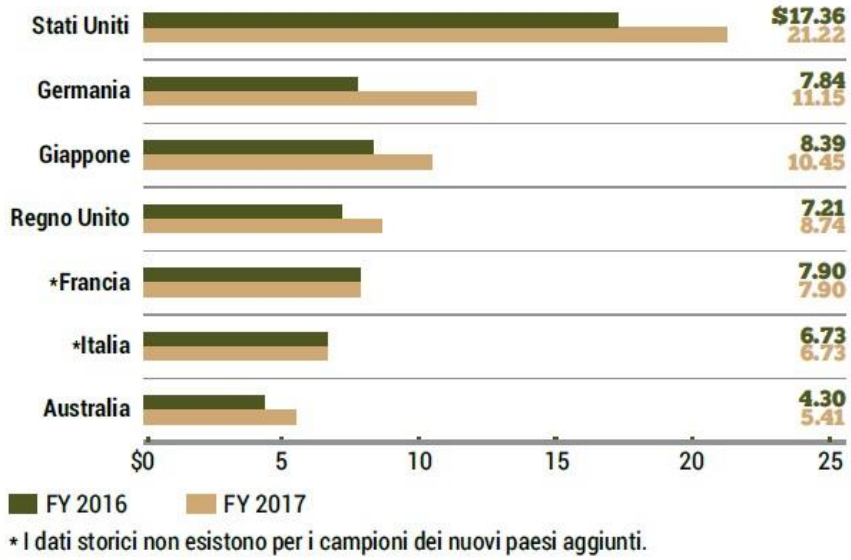
COSTI DEGLI ATTACCHI CYBER IN CONTINUA CRESCITA

2018: il peggiore anno di sempre

GRAFICO 1 CYBER CRIMINE COSTI IN CRESCITA

Costi totali degli attacchi informatici in 7 Stati mondiali - confronto anni 2016-2017

FONTE: ACCENTURE - 2017 COST OF CYBER CRIME STUDY [IN MILIONI DI $ US].

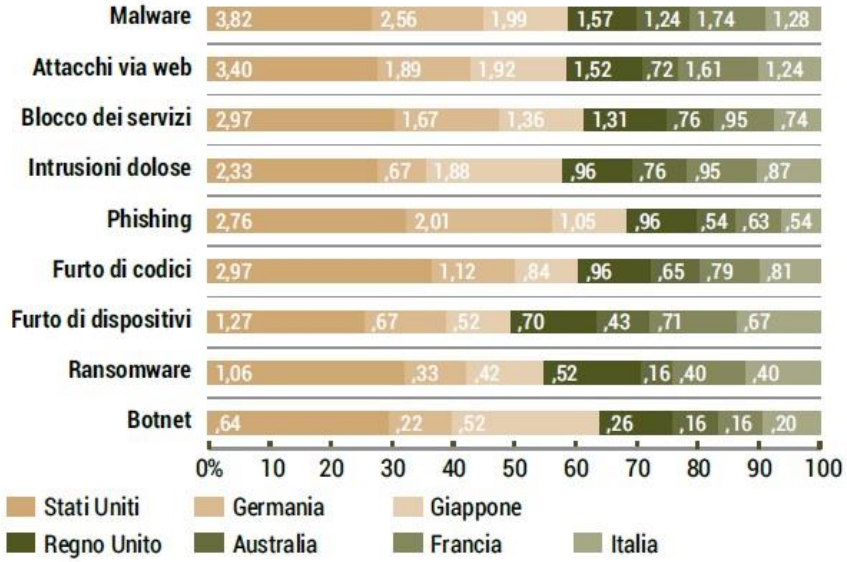


* I dati storici non esistono per i campioni dei nuovi paesi aggiunti.

GRAFICO 2 I COSTI ANNUALI DEGLI ATTACCHI INFORMATICI...

Danni delle varie forme di cybercrimine in 7 Stati mondiali [in milioni di $ Us]

FONTE: COST OF CYBER CRIME STUDY 2017, PONEMON INSTITUTE LLC.



I RISCHI

GDPR; Know-how, Industria 4.0, IoT, Direttiva NIS

- Le aziende tecnologicamente più avanzate, condizione imprescindibile per mantenersi competitivi nel mercato globale, sono gli obiettivi maggiormente attaccabili.
- La sovrapposizione tra uso aziendale e uso personale delle risorse informatiche aumenta i rischi di violazioni.
- Internet, social network e home banking vengono usati in modo sempre più diffuso sia in ambito privato sia in ambito lavorativo.

GLI AGGRESSORI

Criminalità organizzata, professionisti e smanettoni

- Crimine organizzato
- **Insider**
- Spie industriali
- Hacktivist
- Wannabe lamer, script kiddie

LE MINACCE
Non manca proprio nulla

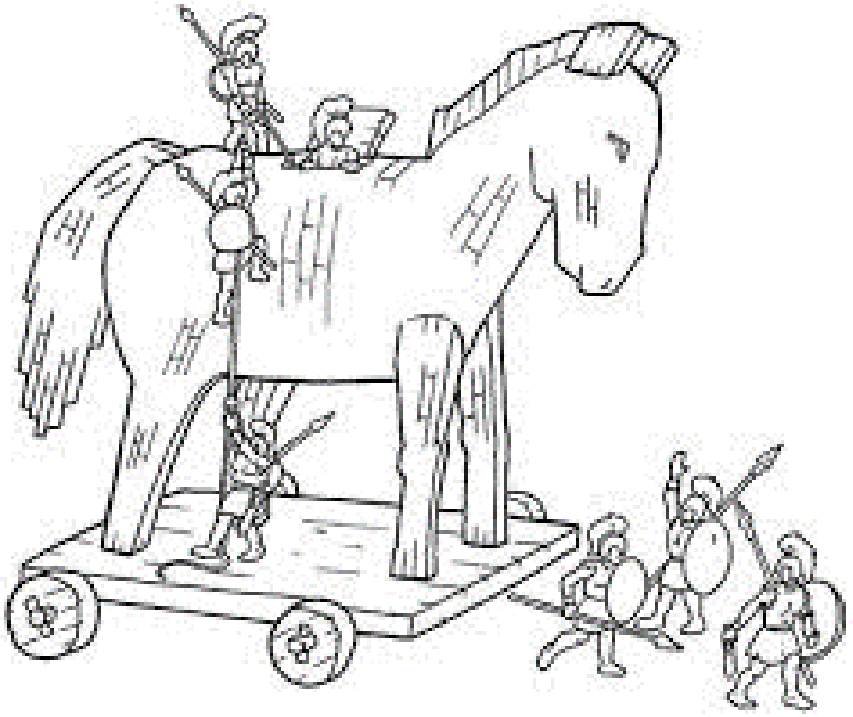
- Frodi
- Furto d'identità
- Furto di dati sensibili e di proprietà intellettuale
- Spionaggio
- Sabotaggio
- Attacchi dimostrativi
- Estorsione/Pizzo elettronico

VULNERABILITA' UMANE

Noi utenti siamo il primo fattore di rischio

La prima breccia nella sicurezza di un sistema si ottiene non con strumenti tecnici, ma semplicemente sfruttando aspetti del comportamento umano:

- distrazione
- superficialità
- negligenza
- altruismo
- fiducia
- curiosità
- ignoranza



LE CONTROMISURE
Informazione e formazine

- Conoscere la minaccia aiuta senza dubbio a mettere in atto semplici azioni che possono impedire di cadere vittima dei più comuni rischi e possono fare la differenza.
- L'aggiornamento costante è fondamentale perché questi strumenti si evolvono ad una velocità esponenziale.

COME MUOVERSI

Gestione del Cyber Risk: il percorso virtuoso

PREVENZIONE

Strumenti di Prevenzione

Impedire il verificarsi - Ritardarne l'accadimento

Analisi:
Information Security Review; Vulnerability Assessment; Penetration Test

Formazione

Monitoraggio e controllo

PROTEZIONE

Strumenti di Protezione

Minimizzarne gli effetti del danno

Misure organizzative:
processi e procedure Incident & Crisis Management

Misure tecniche:
Back-Up; Disaster Recovery IT; soluzioni HD e SW

Misure fisiche:

Sicurezza dei CED

TRASFERIMENTO

Ritenzione del rischio in proprio

Trasferimento del rischio attraverso l'assicurazione per sottrarre l'impresa alle conseguenze finanziarie derivanti dal danno

LA METODOLOGIA ASSITECA

Fasi di intervento

1. Analisi
2. Progettazione
2. Implementazione
3. Monitoraggio

ISR – INFORMATION SECURITY REVIEW

ASSESSMENT TECNICO/ORGANIZZATIVO

- Sicurezza dei sistemi informativi
- livello «maturità»
- Definizione generale interventi
- FOCUS
  - Incident management
  - Continuità operativa

OUTPUT

REPORT ISR

DEFINIZIONE INTERVENTI

- Approfondimento prescrizioni specifiche
- Definizione obiettivi
- Quantificazione risorse e budget
- Analisi possibili criticità

OUTPUT

PIANO DI IMPLEMENTAZIONE

INTERVENTI ORGANIZZATIVI

- Definizione processi gestione IT
- Formalizzazione e applicazione procedure
- Revisione servizi terze parti
- Definizione e attuazione modello di controllo

INTERVENTI INFORMATICI

- Ottimizzazione hardware (HW) – software (SW)
- Selezione nuovi strumenti HW e SW
- Rafforzamento Cyber Security
- Miglioramento continuità Operativa

INTERVENTI INFRASTRUTTURE

- Sicurezza Fisica
- Resilienza infrastrutture fisiche

PMO

- Project Management

OUTPUT

CRONO PROGRAMMA STATO AVANZAMENTO

LIVELLO MATURITA'

- ISR Light periodico

FOCUS REQUISITI INDUSTRIA 4.0 / GDPR / NIS

- Cyber Security
- Protezione dati personali
- Incident management
- Continuità operativa

OUTPUT

REPORT DIAGNOSTICO

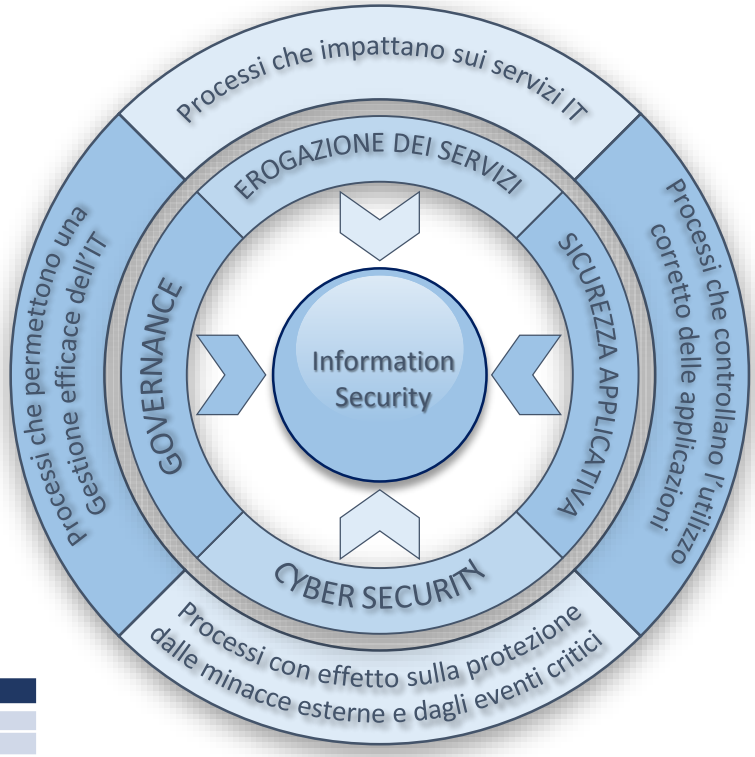
INFORMATION SECURITY REVIEW - ISR

Le caratteristiche

- Servizio offerto agli **IT manager** e all'Alta Direzione.
- Supporto alla definizione di un "programma" organico sulla sicurezza informatica che serva sia come **strumento operativo** per l'IT sia come **documento programmatico** per l'Alta Direzione aziendale. E' molto utile anche per le aziende che affidano gran parte dei loro sistemi a consulenti esterni.
- E' **un'analisi tecnico/organizzativa**, svolta da un nostro esperto in sicurezza informatica, che dopo alcune interviste al personale IT (interno e/o esterno) ed un sopralluogo in azienda predisporrà, in **stretta collaborazione con l'IT**, un **dettagliato report per usi interni** e un **report direzionale** che illustrerà la **situazione attuale della sicurezza** dei sistemi informativi e che indicherà gli **interventi organizzativi** (es. procedure e controlli) e **tecnologici** (es. vulnerability assessment e penetration test) che sarebbe opportuno implementare e/o eseguire nel prossimo periodo.
- I risultati potranno essere **presentati congiuntamente all'Alta Direzione**, permettendo così al referente IT di dare anche maggiore visibilità e concretezza a valutazioni e proposte che sicuramente aveva già iniziato ad elaborare autonomamente.
- L'intervento ha un **costo contenuto** e potrà essere svolto **in poche settimane**, in funzione della disponibilità del personale IT dell'azienda.
- In ambito **GDPR** poi, questo tipo di analisi potrà contribuire alla **riduzione del livello di responsabilità** del Titolare del trattamento dei dati personali perché permetterà di dimostrare che l'organizzazione ha avviato un'analisi generale della sicurezza informatica, come richiesto, ed ha definito i necessari interventi di miglioramento.

INFORMATION SECURITY REVIEW
La metodologia

- Metodologia COBIT 4.1 integrata con ISO 27001 e requisiti GDPR - UE679/2016 e DLGS 196
  - ✓ Dialogo con i responsabili dei sistemi informativi;
  - ✓ Visita alle infrastrutture IT;
  - ✓ Osservazione attività/prassi personale IT;
  - ✓ Studio documentazione IT disponibile;
- 4 aree di analisi che raggruppano **15 specifici macro processi IT** (su 34 totali di COBIT). Rappresentano le **aree** che l'azienda deve presidiare in relazione alla propria sicurezza Informatica;
- Valutazioni (definizioni negli allegati)



LIVELLO DI MATURITA'	
0	Non esistente
1	Iniziale/ad hoc
2	Ripetibile ma intuitivo
3	Definito
4	Gestito e misurabile
5	Ottimizzato

PROBABILITA'		
ALTA	MEDIA	BASSA
A	M	B

IMPATTO		
ALTO	MEDIO	BASSO
A	M	B

CATEGORIE
Danni fisici
Perdita di servizi essenziali
Problemi tecnici
Compromissione di informazioni
Azioni non autorizzate
Problema operativo
Azioni non autorizzate di terzi

OUTPUT

REPORT
INFORMATION SECURITY REVIEW

- Azioni di miglioramento
  - ✓ **Executive Summary** con illustrazione grafica dei contenuti del rapporto di sintesi
  - ✓ **Rapporto di sintesi**;
  - ✓ **Rapporto di dettaglio** con evidenze, suggerimenti e azioni di miglioramento per i Responsabili IT

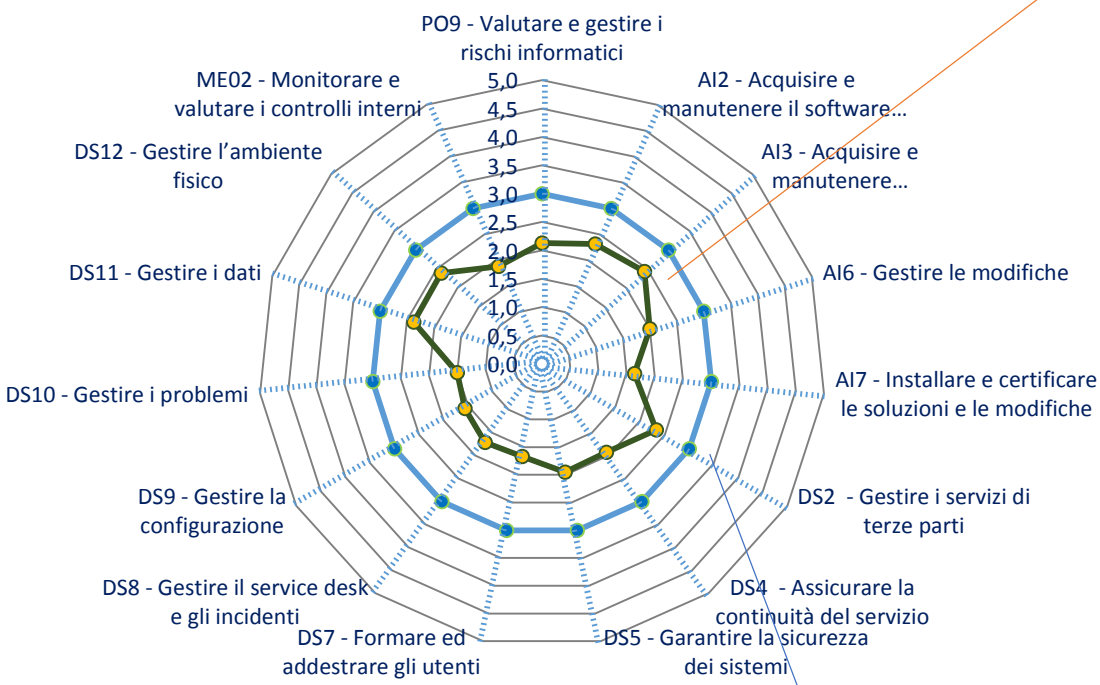
SINTESI DEI RISULTATI

Valutazione dei processi IT

Livello di maturità dei processi esaminati

DS5 - Garantire la sicurezza dei sistemi	1,95
AI3 - Acquisire e manutenere l'infrastruttura tecnologica	2,43
DS9 - Gestire la configurazione	1,57
DS11 - Gestire i dati	2,38
DS12 - Gestire l'ambiente fisico	2,39
Cybersecurity	**2,14**
AI6 - Gestire le modifiche	2,00
AI7 - Installare e certificare le soluzioni e le modifiche	1,64
AI2 - Acquisire e manutenere il software applicativo	2,31
DS7 - Formare ed addestrare gli utenti	1,67
Sicurezza Applicativa	**1,91**
DS2 - Gestire i servizi di terze parti	2,33
DS8 - Gestire il service desk e gli incidenti	1,71
DS10 - Gestire i problemi	1,50
DS4 - Assicurare la continuità del servizio	1,93
Erogazione dei servizi	**1,87**
PO9 - Valutare e gestire i rischi informatici	2,13
ME02 - Monitorare e valutare i controlli interni	1,88
Governance	**2,02**

VALUTAZIONE ATTUALE= 1,99



TARGET = 3,0

LIVELLO DI MATURITÀ					
0	1	2	3	4	5
NON ESISTENTE	INIZIALE / AD HOC	RIPETIBILE MA INTUITIVO	DEFINITO	GESTITO E MISURABILE	OTTIMIZZATO

AZIONI DI MIGLIORAMENTO

Riassunto degli interventi suggeriti

In generale si rileva una significativa carenza di formalizzazione dei processi che sono affidati quasi sempre alle prassi in essere e spesso privilegiano l'immediatezza a scapito di elementi di sicurezza e di controllo ex-post. Questo rende i processi soggetti ad interpretazioni diverse in base all'esperienza e a continui aggiustamenti al variare delle situazioni. In particolare, risultano migliorabili nella gestione delle interazioni tra strutture aziendali diverse, con gli utenti e nel coinvolgimento in nuovi progetti fin dalle fasi preliminari.		**PRIORITA' ALTE e MEDIO-ALTE**
CYBERSECURITY	• Migliorare i **Disciplinari** e implementare misure di prevenzione e controllo • Effettuare **un'analisi dei rischi del sito web** • Migliorare la **gestione di utenze e abilitazioni** e fare **verifiche periodiche** • **Segmentare maggiormente la rete** ai fini della protezione delle risorse critiche • Migliorare le **misure di sicurezza** e implementare regolari attività di **Vulnerability Assessment**	**A1, A2, A3, A4, A7, A8, A11, A14**
SICUREZZA APPLICATIVA	• Migliorare e formalizzare la procedura di **Rilascio in Produzione** • Migliorare e formalizzare i processi **di Change e Demand Management** (ad es. tracciatura completa degli interventi) • Assicurare un efficace processo di **trasferimento della conoscenza**	**A17**
EROGAZIONE DEI SERVIZI	• Strutturare meglio il processo di **Incident e Problem Management** • Rafforzare l'impianto di **Condizionamento del Data Center** • Coinvolgere maggiormente **l'Area Infrastrutture** nei progetti strategici (ad es. Magazzino automatizzato) • Implementare una soluzione di **Disaster Recovery** • Adeguare l'**impiantistica del Data Center** • Eseguire una **Business Impact Analysis** (BIA); formalizzare le procedure per la continuità operativa e definire e formalizzare una soluzione di Disaster Recovery minimale	**C1, C2, C3, C4, C7**
GOVERNANCE	• Migliorare **l'Analisi dei Rischi** (ad es. individuazione puntuale delle contromisure) • Inserire, nei vari processi, opportune attività di **verifica** periodica e di gestione delle eccezioni • Implementare un **processo di misurazione e comunicazione delle attività svolte**, dei servizi erogati e delle verifiche effettuate • Migliorare **la tracciatura delle attività degli Amministratori** di Sistema	**D1, D2, D3**

PROGETTAZIONE
Definizione interventi

Approfondimento dei contenuti

- Risk Analysis - Probabilità/Impatto
- Verifica requisiti di conformità

Definizione obiettivi

- Interventi
- Priorità temporali
- Definizione personale interno esterno necessario

Quantificazione risorse e budget

- Definizione personale interno esterno necessario
- Quantificazione costi di implementazione

Analisi possibili criticità

- Sovrapposizione progetti
- Difficoltà esecutive
- Efficacia interventi

Predisposizione piano di implementazione

- Piano di intervento
- Crono programma con attività e milestone

OUTPUT

PIANO DI IMPLEMENTAZIONE

IMPLEMENTAZIONE 1/2
Interventi organizzativi e PMO

INTERVENTI ORGANIZZATIVI

- **Definizione dei processi** di gestione dei sistemi informativi
  - **Incident Management** e **notifica** eventi critici

OUTPUT
TUTORING
DIAGRAMMI e WORKLOW

- **Formalizzazione e applicazione procedure**

OUTPUT
PROCEDURE

- **Revisione servizi** terze parti (fornitori IT)
  - Obblighi e clausole contrattuali sulla sicurezza

OUTPUT
CONTRATTUALISTICA

- Definizione e attuazione **modello di controllo**
  - **Reportistica** da personale IT e Fornitori IT a Management

OUTPUT
REPORTISTICA

PMO

- Project Management
  - **Supervisione** di progetti specifici
  - **Verifica** scadenze e budget
  - **Escalation** verso Management a fronte di difficoltà di esecuzione

OUTPUT
CRONO PROGRAMMA e STATO AVANZAMENTO

IMPLEMENTAZIONE 2/2

Interventi informatici e fisici

INTERVENTI INFORMATICI

- **Analisi esigenze** di ottimizzazione dell'hardware (HW) e del software (SW)
- **Selezione nuovi strumenti** HW e SW
- Rafforzamento **Cyber Security**
  - Check-up delle reti e dei sistemi informativi
  - Attività di sicurezza logica: Vulnerability assessment; Penetration test;
  - Formazione utenti e esercitazioni

OUTPUT
HW/SW
VENDOR SELECTION

- **MIGLIORAMENTO CONTINUITÀ OPERATIVA**
  - BIA – Business Impact Analysis
  - Predisposizione procedure di backup e verifica procedure di ripristino
  - Predisposizione di piani di Disaster Recovery IT

OUTPUT
PROCEDURA DI BACKUP
DISASTER REVOVERY PLAN

INTERVENTI INFRASTRUTTURE

- Verifica e incremento della Sicurezza Fisica del CED (Centro Elaborazione Dati)
- Valutazione resilienza infrastrutture IT (LAN/WI-FI e TLC)

OUTPUT
ASSESSMENT
ISPEZIONI

MONITORAGGIO

Controllo resilienza IT e requisiti GDPR/NIS/INDUSTRIA 4.0/PROTEZIONE KNOW-HOW

LIVELLO MATURITA'

- DIAGNOSTICO SICUREZZA INFORMATICA - DSI
  - Attuazione interventi implementazione
  - Nuove esigenze operative
  - Evoluzione requisiti normativi

REQUISITI INDUSTRIA 4.0

- CYBER SECURITY
- CONTINUITA' OPERATIVA
  - Esercitazioni
  - Test DR

REQUISITI GDPR

- PROTEZIONE DATI PERSONALI
- GESTIONE RICHIESTE E DIRITTI INTERESSATI

REQUISITI NIS

- INCIDENT MANAGEMENT
  - Verifica livello attuazione processo
  - Notifica

OUTPUT

REPORT DIAGNOSTICO

VANTAGGI OPERATIVI
della Sicurezza Informatica

- **Valutazione approfondita** dello stato attuale di **maturità** della sicurezza informatica in termini di gestione dei **Rischi Informatici, misure di sicurezza logica** previste**, modalità di protezione dell'ambiente fisico, modalità di controllo** adottate
- Maggiore **consapevolezza dell'importanza dei sistemi informativi** per la generazione di valore in azienda
- Individuazione dei **principali rischi** (findings), delle eventuali **azioni necessarie** a minimizzarli, dei tempi e del budget necessari alle relative implementazioni
- Riduzione dei rischi di **violazioni** interne e esterne, la **perdita di dati** (informazioni riservate, progetti etc.) e **interruzioni produttive**
- Limitazione delle attività di **spionaggio** interno o della concorrenza
- Maggiore difesa da **virus** e organizzazioni criminali (**hacker**)
- Adeguamento alle **normative** (GDPR, NIS, INDUSTRIA 4.0, ISO 9001, etc) e **riduzione accountability**
- Ottimizzazione delle **coperture assicurative** (Cyber Risk, Business Interruption, D&O, Legal)

IN CONCLUSIONE

Sicurezza Informatica per tutti !

Emanuele Capra

Senior Consultant – Assiteca Consulting Srl
emanuele.caprai@assiteca.it

Francesco Manzo

Responsabile Filiale di Salerno – Assiteca SpA
francesco.manzo@assiteca.it

ASSITECA S.p.A.
Via Fratelli de Mattia 6 - Salerno
www.assiteca.it