Cos’è un ransomware e come difendersi, il vademecum del Garante Privacy

Cos’è un ransomware e come ci si difende da questa truffa online, che infetta pc, smartphone e tablet per chiedere poi un riscatto per liberarli? Il **Garante Privacy** ha pubblicato un vademecum per spiegare nel dettaglio cos’è un ransomware e come comportarsi per evitare l’infezione e per liberare il device nel caso di rapimento, confisca e blocco del device come nei casi recenti più eclatanti di Bad Rabbit, Petya e Wannacry.

Il ransomware è un programma che infetta i dispositivi elettronici e chiede un riscatto (ransom significa riscatto in inglese) per lo più in bitcoin per liberare i contenuti (fino a 200-300 dollari nel caso di Bad Rabbit).

La prima difesa è “evitare di aprire messaggi provenienti da soggetti sconosciuti e con i quali non si hanno rapporti”, si legge nella guida del Garante, che fra le prime contromosse consiglia l’uso di antivirus, freqeunti aggiornamenti e backup.

Evitare di aprire mail, sms, chat e messaggi sospetti e di aprire allegati o cliccare link o banner in essi contenuti. Un dispositivo infettato può, purtroppo, contaghiare i contatti della rubrica e diffondere così il virus online.

Pagare il riscatto non è la soluzione, la prima cosa da fare è denunciare l’attacco alla Polizia Postale e rivolgersi a tecnici specializzati.



ATTENZIONE AL RANSOMWARE

Il programma che prende «in ostaggio» PC e smartphone

1. COS'E' IL RANSOMWARE?

Il **ransomware** è un programma informatico dannoso che infetta un dispositivo (PC, tablet, smartphone, smart TV), **bloccando l'accesso ai contenuti** (foto, video, file) e **chiedendo un riscatto** *(in inglese, ransom)* per «liberarli». La **richiesta di pagamento** con le relative istruzioni è presentata in una finestra che appare automaticamente sullo schermo del dispositivo infettato. L'utente ha pochi giorni per pagare: **poi il blocco diventa definitivo.** Ci sono **due tipi principali di ransomware**: i **cryptor** (che criptano i file contenuti nel dispositivo rendendoli illeggibili) e i **blocker** (che bloccano l'accesso al dispositivo infettato).

2. COME SI DIFFONDE?

Il ransomware si diffonde soprattutto attraverso **messaggi** - inviati via e-mail, sms o chat o che appaiono su pagine web e social network - che sembrano provenire da **soggetti conosciuti e sicuri** come corrieri espressi, gestori di servizi *(acqua, luce, gas)*, operatori telefonici, soggetti istituzionali, ecc.. Chi li riceve è indotto ingannevolmente ad **aprire allegati** o a **cliccare link o banner** collegati a software dannosi. Il dispositivo infettato può poi «contagiarne» altri, perché il ransomware, impossessandosi della **rubrica dei contatti**, può utilizzarla per **spedire automaticamente messaggi contenenti file dannosi.**



3. COME DIFENDERSI?

La prima difesa è **evitare di aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti** *(ad es. un operatore telefonico di cui non si è cliente, un corriere espresso da cui non si aspettano consegne, ecc.)* e **non cliccare su collegamenti a siti sospetti.**
E' utile installare un **antivirus** con estensioni per malware sui propri dispositivi e **mantenere aggiornato il sistema operativo.**
E' fondamentale effettuare **backup periodici dei contenuti:** così, nel caso in cui fosse necessario formattare il dispositivo per sbloccarlo, **i dati in esso contenuti non verranno persi.**

4. COME LIBERARSI DAL RANSOMWARE?

Pagare il riscatto è solo apparentemente la soluzione più facile. Oltre al danno economico, si corre infatti il rischio di **non ricevere i codici di sblocco**, o addirittura di finire in **liste di «pagatori»** potenzialmente soggetti a periodici attacchi ransomware. L'alternativa è quella di **rivolgersi a tecnici specializzati** capaci di sbloccare il dispositivo. Oppure si può **formattare il dispositivo**, ma con il rischio di perdere tutti i dati in esso contenuti se **non è disponibile un backup.**
E' consigliabile sempre segnalare o denunciare l'attacco ransomware alla Polizia postale, anche per aiutare a prevenire ulteriori truffe.

La scheda ha mere finalità divulgative

https://www.key4biz.it/cose-un-ransomware-difendersi-vademecum

-del-garante-privacy/207775/

Ecommerce, a Natale viaggi e hi-tech sotto l’albero. Ma un consumatore su due teme frodi online

Una nuova indagine condotta tra Europa e Stati Uniti rivela che oltre **il 45% dei consumatori teme di acquistare involontariamente prodotti contraffatti in rete**. Uno su tre denuncia di essere stato già ingannato e di averne comprati.

Sono i dati relativi all’indagine MarkMonitor sugli acquisti online, “***Global Online Shopping Survey 2017 – Counterfeiting Concerns***”, che ha coinvolto quasi 3.500 persone, con il fine di realizzare una panoramica sulla contraffazione. Lo scopo dell’indagine è stato quella di valutare gli atteggiamenti e le esperienze online dei consumatori, su come agiscono acquistando sul web, se comprano consapevolmente prodotti contraffatti, quali canali prediligono e se si pongono problemi di sicurezza.

Nel 34% dei casi di prodotti contraffatti acquistati online, gli intervistati hanno dichiarato di essere stati frodati tra due e tre volte. **Il 63% ha paura di comprare prodotti contraffatti soprattutto per i bambini. In Italia tale dato sale all’86%.**

L’85% dei consumatori chiede ai brand di fare di più per contrastare il **fenomeno, che lo ricordiamo nel 2016 ha consentito a gruppi di cyber criminali di guadagnare oltre 460**

miliardi di dollari.

Nonostante questo, i consumatori rimangono fiduciosi nel mezzo internet e il 47% di loro continua a fare shopping online, il 56% via smartphone. Lo scorso anno gli acquisti online in Gran Bretagna hanno generato una spesa complessiva di 133 miliardi di sterline, negli USA 395 miliardi di dollari, con un balzo in avanti del 16% sul 2015.

Per quanto riguarda i consumatori italiani, in vista del Natale 2017, una nuova indagine di *Speedvacanze.it* ha rivelato che la gran parte spera di **ricevere in dono soprattutto viaggi, indicati dal 21% del campione, regali tecnologici (19%)**, orologi, penne e gioielli (18%) e capi di abbigliamento e accessori (16%). Ma anche profumi (nominati dal 12% degli interpellati), libri e calendari (7%) e prodotti enogastronomici (4%).

Sempre più persone quindi fanno affidamento sulla tecnologia per acquistare regali, cibo e abbigliamento; infatti, secondo un altro studio condotto da Deloitte, **l'83% dei consumatori quest'anno intende acquistare online spendendo circa 228 dollari in più a famiglia rispetto al 2016.**

Secondo la ricerca di Kaspersky Lab però, a causa dei criminali informatici che prendono di mira i dispositivi, gli utenti rischiano di dover aggiungere un costo di 636 dollari alla spesa per lo shopping natalizio per il costo medio di recupero dei dati rubati o danneggiati.

Purtroppo, nonostante i pericoli e i potenziali rischi per i dati, la ricerca mostra che solo la metà dei consumatori effettua il backup dei propri dati e **il 34% di loro ammette di non effettuare il backup online. Questo comportamento, nel peggiore dei casi, potrebbe lasciare molti consumatori al verde** e senza la possibilità di accedere ai propri dati durante il periodo natalizio. Ma c'è un modo semplice per evitare questo problema: il backup regolare dei dati e

l’introduzione di misure di sicurezza potenziate che garantirebbero ai consumatori tranquillità per tutto l’anno, assicurando la protezione delle informazioni.

> *Ecommerce, a Natale viaggi e hi-tech sotto l’albero. Ma un consumatore su due teme frodi online*

Digitanomalie. Come funziona veramente la Differential Privacy di Apple

Learning with Privacy at Scale *è* un documento redatto dal ***Differential Privacy Team*** di **Apple** che spiega in termini comprensibili (?) i presupposti matematici della raccolta e del trattamento dei dati relativi a come le persone usano **Ipad**, **Iphone** e **Macbook**.

Benchè seduttivamente intitolato utilizzando la parola “privacy” questo metodo matematico ha poco a che vedere – in sè – con la tutela della riservatezza perché il suo obiettivo è impedire di conoscere il valore di verità di una singola informazione, pur conservando – su scala aggregata – il valore statistico dei risultati.

In pratica, immaginiamo di chiedere a un certo numero di persone (selezionato in modo da costituire un campione statisticamente valido) di esprimere l’intenzione di voto.

E’ intuitivo che, a livello aggregato non sia possibile sapere “chi” vota per “chi”, ma conservando i dati grezzi (i risultati individuali del questionario) questa associazione è

sempre possibile.

Per ovviare a questo problema, il metodo matematico rispolverato da Apple prevede che già a livello di raccolta del dato, tramite l'introduzione controllata di errori, non sia possibile sapere se la risposta associata alla singola persona sia vera o falsa, pur conservandosi il valore statistico dell'analisi aggregata.

Come è facile vedere, ciò che viene chiamato "Differential Privacy" non garantisce, in sè, la tutela della riservatezza ma solo l'impossibilità di conoscere con certezza se un certo dato sia effettivamente riferibile a una specifica persona.

Per di più, se la domanda è stata posta in modo mirato – ad esempio: "nello schieramento X, voterai per A o per B?" – il meta risultato dell'orientamento politico del singolo intervistato rimane intatto. Tanto è vero questo che il documento di Apple si prende la briga di dichiarare che *The records arrive on a restricted-access server where IP identifiers are immediately discarded, and any association between multiple records is also discarded.* Cioè che i dati, già "inoculati" con errori casuali sul terminale dell'utente, vengono anonimizzati non appena arrivano sui server dell'azienda di **Cupertino**.

Come volevasi dimostrare, dunque, la *Differential Privacy* – se non è affiancata da tecniche di anonimizzazione – non garantisce la tutela di ciò che giuridicamente qualifichiamo come riservatezza dello spazio personale.

Resta da chiedersi il perché dell'utilizzo della parola "privacy" in un contesto nel quale questo istituto giuridico ha una rilevanza relativa e, soprattutto, quando ci si rivolge a un pubblico di non matematici.

Non è "colpa" di Apple perché la nozione di "Differential Privacy" è stata elaborata già a partire dal 2006. Ma rimane il problema dei rischi di una comunicazione scientifica non

rigorosa.

E’ molto, troppo elevato il rischio che il legislatore e le autorità di controllo possano essere indotti in errore, approvando leggi sbagliate e applicandole in modo errato.

> *Digitanomalie. Come funziona veramente la Differential Privacy di Apple*

Cybersecurity, a Roma 297mila dispositivi a rischio attacco hacker

A **Roma** sono 296.786 i dispositivi a rischio attacco cyber e, se si sommano i sistemi a rischio presenti nelle capitali dell’Europa occidentale, si arriva a un totale che supera i 10 milioni.

Tra i dispositivi a rischio si contano 217.109 web service, 2.890 email service, 2.595 webcam, 432 MySQL database, 154 router, 79 dispositivi VoIP e 29 registratori media. Questo è quello che emerge dall’ultimo report “Western European Cities Exposed” di Trend Micro.

Lo studio ha analizzato i cosiddetti “sistemi esposti” di 2,7 milioni di indirizzi IP in 10 capitali europee: Amsterdam, Atene, Berlino, Lisbona, Londra, Madrid, Oslo, Parigi, Roma e Stoccolma, ovvero quei dispositivi collegati a Internet che rispondo alle richieste sia tramite strumenti di gestione della rete o di enumerazione, come un ping, o che possono essere trovati da motori di ricerca internet come Shodan o

simili. Non sono per definizione vulnerabili o compromessi, ma il fatto che siano connessi significa che possono essere attaccati in qualunque momento.

I dispositivi esposti offrono ai possibili attaccanti una radiografia di come i dispositivi stessi sono utilizzati dalle aziende e dai governi, questo può facilitare le operazioni di infiltrazione nella rete. I sistemi connessi a Internet spesso restano aperti a potenziali attacchi o perdite di dati perché non sono configurati correttamente. Tuttavia, alcuni devono essere connessi per forza a Internet, per poter funzionare correttamente o per abilitare l'accesso remoto per la risoluzione dei problemi e altre attività. I dispositivi a rischio possono provocare una fuga di informazioni private all'insaputa dell'utente, permettere il furto di dati critici aziendali e governativi, essere sfruttati per attacchi mirati o attacchi DDoS e anche essere presi in ostaggio nel corso di un attacco ransomware.

Per quanto riguarda la tipologia dei dispositivi, lo studio ha rivelato che nelle città esaminate sono a rischio, in totale, 58.000 punti di accesso wireless, 34.000 firewall e 28.000 webcam. Inoltre è stato rilevato un grande numero di stampanti accessibili pubblicamente da internet, che mettono potenzialmente a rischio le copie di dati sensibili, così come offrono agli attaccanti un punto per entrare all'interno delle reti aziendali. I sistemi operativi esposti maggiormente sono Linux (62%) e Windows (20%).

Questo studio deve essere tenuto in particolare considerazione, anche in relazione all'entrata in vigore del **nuovo Regolamento Europeo sulla protezione dei dati (GDPR)**. I dispositivi a rischio innalzano infatti il rischio di subire una violazione di dati, severamente punita dal regolamento.

Natale 2017, aumentano gli attacchi DDoS e la vulnerabilità dei POS

Natale è alle porte e come ogni anno ormai si inizia a studiare la strategia migliore e più efficace per prevenire gli attacchi informatici e allo stesso tempo limitarne i danni a imprese e consumatori. Perché Natale è il periodo dell'anno dove si spende di più e soprattutto lo si fa online, dove si annidano i cyber criminali.

L'ammontare delle operazioni fatte tramite POS (*Point-Of-Sales*) vale oggi complessivamente circa 160 miliardi (nel 2014 circa 79 miliardi), mentre altri 30 miliardi sono generati da transazioni relative a prodotti, servizi, bollette, multe e altro veicolato tramite Pc, tablet, smartphone e *POS contactless*.

A questi, secondo gli ultimi dati dell'Osservatorio Mobile Commerce & Payment del Politecnico di Milano, va aggiunto anche il **POS mobile**. L'anno scorso ne sono stati attivati 85 mila, il 20% in più rispetto al 2015.

Da una nuova indagine è emerso che **negli ultimi 12 mesi è stato rilevato un notevole aumento del 16% degli attacchi di tipo DDoS (*Distributed Denial of Service*)**, mentre sono in rapido aumento anche gli attacchi che sfruttano le **vulnerabilità dei sistemi POS**.

Questo significa, per i ricercatori Kaspersky Lab, che qualunque cosa stiano pianificando i cybercriminali in questo periodo, è molto probabile che per gli attacchi che ci saranno durante le lunghe festività natalizie utilizzeranno proprio

queste due tipologie di violazione.

“*Tenuto conto che nell’ultimo anno è stato rilevato un considerevole aumento di questo tipo di attacchi, raccomandiamo alle aziende – in particolare ai retailer – di prestare maggiore attenzione durante il periodo natalizio, poiché è più alta la possibilità per i criminali informatici di fare affari redditizi sfruttando i sistemi di pagamento o gli attacchi DDoS*”, ha dichiarato in una nota **Morten Lehn**, General Manager Italy di Kaspersky Lab.

“*Questi attacchi consentono ai criminali informatici di chiedere un riscatto o semplicemente impedire a un’azienda di offrire i propri servizi favorendo la perdita di guadagni e clienti*”.

Tra luglio e settembre del 2017, rileva uno studio Akamai, la situazione è peggiorata sotto ogni punto di vista. Sono cresciuti gli attacchi DDoS, sia su base trimestrale sia su base annuale; **aumenta l’attività delle botnet**; gli attacchi rivolti alle applicazioni web hanno visto un’impennata inattesa e alquanto preoccupante.

Gli attacchi DDoS sono cresciuti in quantità, ma la loro portata (in senso di “potenza di fuoco”) si è notevolmente ridotta rispetto a quelli della seconda metà del 2016. Nel terzo trimestre 2017, **gli attacchi *Distributed Denial of Service* sono cresciuti dell’8% su base trimestrale, mentre il numero di attacchi medi nei confronti di ogni singola vittima sono aumentati del 13%** (ogni obiettivo ha subito una media di 36 attacchi nel trimestre, ovvero uno ogni tre giorni circa).

Digitanomalie. Il Governo disciplina i database di polizia, ma sbaglia la norma di riferimento

Dopo la clamorosa e gravissima "fuga in avanti" del Parlamento che, ignorando la delega attribuita al Governo per modificare il Codice dei dati personali, ha approvato una norma che rischia di paralizzare la ricerca medica e la sperimentazione clinica, è la volta del Governo di "legiferare" in modo incoerente sul trattamento dei dati personali e sull'applicazione del **GDPR**.

Nel Comunicato stampa del Consiglio dei Ministri n. 60 del 01 Dicembre 2017, infatti, il Governo ha annunciato di avere approvato un regolamento sulle "*modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia*".

Ma il Considerando numero 16 del GDPR stabilisce che:

Il presente regolamento ***non si applica*** *a questioni di tutela dei diritti e delle liberta` fondamentali o di libera circolazione dei dati personali riferite ad attivita` che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le* ***attivita` riguardanti la sicurezza nazionale****. Il presente regolamento non si applica al trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attivita` relative alla politica estera e di sicurezza comune dell'Unione.*

Dunque le attività di pubblica sicurezza – quelle di cui si occupa il provvedimento governativo – dovrebbero, si essere

normate. Ma ai sensi eventualmente della direttiva 680/2016 (relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali) e non del GDPR.

Peccato che, però, la direttiva in questione non sia stata ancora recepita.

C'è da sperare che, nell'attuazione della delega ricevuta per armonizzare Codice dei dati personali e GDPR il Governo manifesti più attenzione.

Il rischio che da Regolamento Generale si passi ad Anarchia Sistematica è dietro l'angolo.

Natale 2017, attesi 50 milioni di cyberattacchi. Phishing in crescita del 74%

I recenti *Blackfriday* e *Cybermonday* sono ormai da qualche anno considerati gli eventi apripista del lungo periodo delle feste natalizie. E proprio in occasione di questi giorni di shopping intenso, sia in store che online, il pericolo di frodi e attacchi informatici raggiunge i massimi livelli.

I computer infettati da malware negli Stati Uniti sono aumentati mediamente di oltre il 123%, secondo i nuovi dai Enigma Software Group. Nello specifico, **+110% durante il *Blackfriday***, +119% e +127% rispettivamente i successivi sabato e domenica e **+137% in occasione del cybermonday**.

È stata stilata anche una **classifica delle città più colpite dai malware nel "*Thanksgiving weekend*"** (fine settimana del Giorno del Ringraziamento), che vede Charlotte al primo posto con un incremento degli attacchi informatici del 316%, seguita da Detroit con un +275%, quindi **New York con +237%,** Salt Lake City +212%, Sacramento +210%.

L'attenzione ora si sposta inevitabilmente alle ultime settimane dell'anno, quelle che sostanzialmente precedono le feste natalizie vere e proprie. Secondo il nuovo ***Cybercrime Report*** di ThreatMetrix, in tutto il mondo sono **attesi più 50 milioni di cyber attacchi per il Natale 2017**.

In particolare, i Paesi dove le transazioni finanziarie saranno maggiori e con un alto numero di mobile users potrebbero essere tra i principali obiettivi di attacchi. Al contempo, il trimestrale Threat Intelligence Report rilasciato la scorsa settimana da NTT Security rivela che **gli attacchi globali di phishing sono cresciuti in modo preoccupante del 74% nel terzo trimestre del 2017**.

È stato calcolato che ogni attacco di questo tipo crea danni economici alle organizzazioni di medie dimensioni per 1,6 milioni di dollari e nel 2016 gli attacchi di phishing sono cresciuti del 70%.

I danni economici calcolati da Dimension Data per i consumatori che a Natale vorranno fare acquisti online si aggirano tra i 50 ed i 5.000 dollari. Un dato plausibile vista la gran quantità di dispositivi elettronici connessi in rete con i quali si accede alle piattaforme di ecommerce da ogni parte del mondo: Statista calcola che nel 2017 saranno 1,66 miliardi i consumatori di tutto il mondo che faranno almeno un acquisto online, mentre nel 2021 saranno 2,14 miliardi .

Generalmente, ricorda una statistica Barclays, solo nel Regno Unito in occasione delle festività natalizie sono portate a termine oltre un quarto del totale delle truffe online.

Tutti o quasi gli attacchi informatici in questione vogliono solo due cose: i dati delle carte di credito e spendere tutti i soldi sul conto dei poveri malcapitati. Inoltre, i cyber criminali spesso mirano alle informazioni sull'identità personale, come username, password e informazioni contenute sui siti visitati regolarmente. Se un cyber criminale riesce ad accedere alle credenziali personali, potrà utilizzarle su molteplici siti e piattaforme spacciandosi per l'utente frodato.

Per evitare di cadere vittime di frodi informatiche, oltre che disporre di software di sicurezza sempre aggiornati, si possono mettere in pratica comportamenti generali di attenzione alla sicurezza che in molti casi permettono di prevenire i cyber attacchi, come ad esempio utilizzare password ad alto livello di sicurezza (mai le stesse per più siti, mai quelle più banali), non utilizzare mai reti WiFi pubbliche per effettuare acquisti online, oppure non aprire email, non cliccare su link o aprire allegati provenienti da fonti sconosciute, non condividere mai username, password o altre informazioni personali online, diffidare di email indesiderate che promettono offerte entusiasmanti e non aprire i relativi allegati, assicurarsi l'aggiornamento costante dei sistemi di antivirus e patching sui propri dispositivi.

Cybersecurity, mercato da 205 miliardi di dollari nel 2025. Imprese più esposte agli

attacchi con cloud e IoT

Saranno soprattutto le imprese e le banche a far crescere l'industria della ***cyber* sicurezza** in tutto il mondo, facendo lievitare la domanda di servizi e prodotti per la sicurezza informatica a tutto tondo. Solo nel primo semestre di quest'anno, **gli attacchi informatici sono aumentati di oltre l'8% a livello globale**.

L'anno scorso l'intero settore delle **tecnologie per la cybersecurity** ha raggiunto il valore approssimativo di 76,4 miliardi di dollari, ma secondo il Rapport "***Cyber Security Market: Global Industry Analysis and Forecast 2017-2025***", di Persistence Market Research (PMR), nel 2025 tale mercato crescerà ad un tasso annuo (Carg) del 12% per toccare i **205,8 miliardi di dollari**.

A spingere in alto il settore della *cyber* sicurezza saranno soprattutto le nuove piattaforma di servizi *cloud* a livello industriale e aziendale, per i *backu*p, l'*email service*, l'Erp (*Enterprise resource planning*), il Crm (*Customer relationship management*) e i servizi di *collaboration*.

Solo il Nord America vedrà nel 2025 potrebbe rappresentare un mercato di tecnologie per la cybersecurity superiore ai 67 miliardi di dollari, un terzo del totale.

Nell'ultimo anno, più del 50% delle organizzazioni nel mondo, secondo l'ultimo Rapporto Clusit, ha subito almeno un cyber attacco di una certa gravità.

Sono **aumentati del 126% gli attacchi di *cyber* spionaggio, del 23% alle infrastrutture critiche, del 12% alle banche e altri Istituti finanziari** e del 253% quelli definiti "*Multiple targets*", cioè compiuti da uno stesso attaccante e portati avanti in parallelo contro numerosi obiettivi di varia natura.

Se le motivazioni sono sempre le stese (estorcere denaro,

causare un danno economico e di mercato, sottrarre informazioni sensibili e strategiche, le cause invece sono da rinvenire nella solita sottostima dei rischi e nei mancati investimenti in soluzioni di *cybersecurity*.

A questi elementi chiave va aggiunto un più ampio panorama di attività su cui i cyber criminali possono lavorare, frutto di una trasformazione digitale dell'esistente che certamente accrescere la "superficie esposta agli attacchi" della nostra società, dei mercati, delle infrastrutture: la rapida diffusione **di smart working**, che si avvale di strumenti quali **mobile, cloud e social**, spesso utilizzati in maniera indiscriminata mescolando profili personali e lavorativi, e dell'***Internet of Things,*** con apparecchiature per lo più prive delle più elementari misure di sicurezza, costituiscono punti di accesso sempre più immediati verso i sistemi informativi delle organizzazioni.

Da evidenziare che ciò avviene oggi anche in contesti produttivi, quali l'***Industry 4.0***, e per applicazioni critiche come ***ehealth*** e ***smartcity***.