CONSIGLIO NAZIONALE INGEGNERI

C3i COMITATO ITALIANO INGEGNERIA INFORMAZIONE

Gli strumenti e le buone pratiche per difendersi dagli attacchi informatici

Ing. Mattia Siciliano
Ordine Ingegneri della Provincia di Napoli

GdL Cyber Security

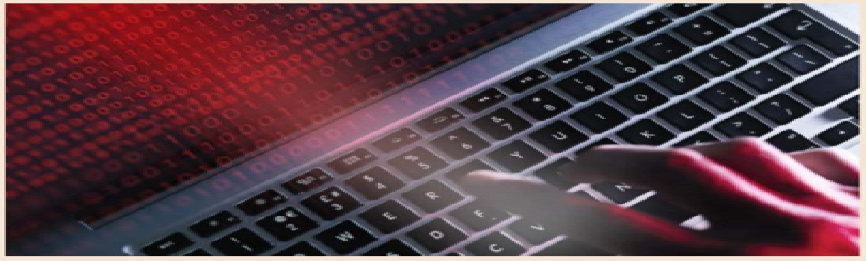
“The objective is to provide an ecosystem that balances the imperative to protect the enterprise with the need to adopt innovative, risky new technology approaches to remain competitive,”

– ***Gartner Rethink the Security & Risk Strategy 2019***

Secondo la società d’analisi MarketsandMarkets, l’industria della cyber-security potrebbe salire a oltre 248 miliardi nel 2023. Questo presuppone **un tasso di crescita annuale del 10,2% nei prossimi cinque anni**.

Gli attacchi informatici costano 8 milioni di dollari alle aziende in Italia

di Luca Tremolada



2' di lettura

In Italia il costo medio annuo per azienda delle violazioni della sicurezza informatica ha raggiunto gli 8 milioni di dollari (13 milioni di dollari per azienda a livello globale), con un incremento del 19% nel 2018 (12% a livello globale). È quanto emerge dal nono studio annuale di Accenture Security sui costi del cybercrime.

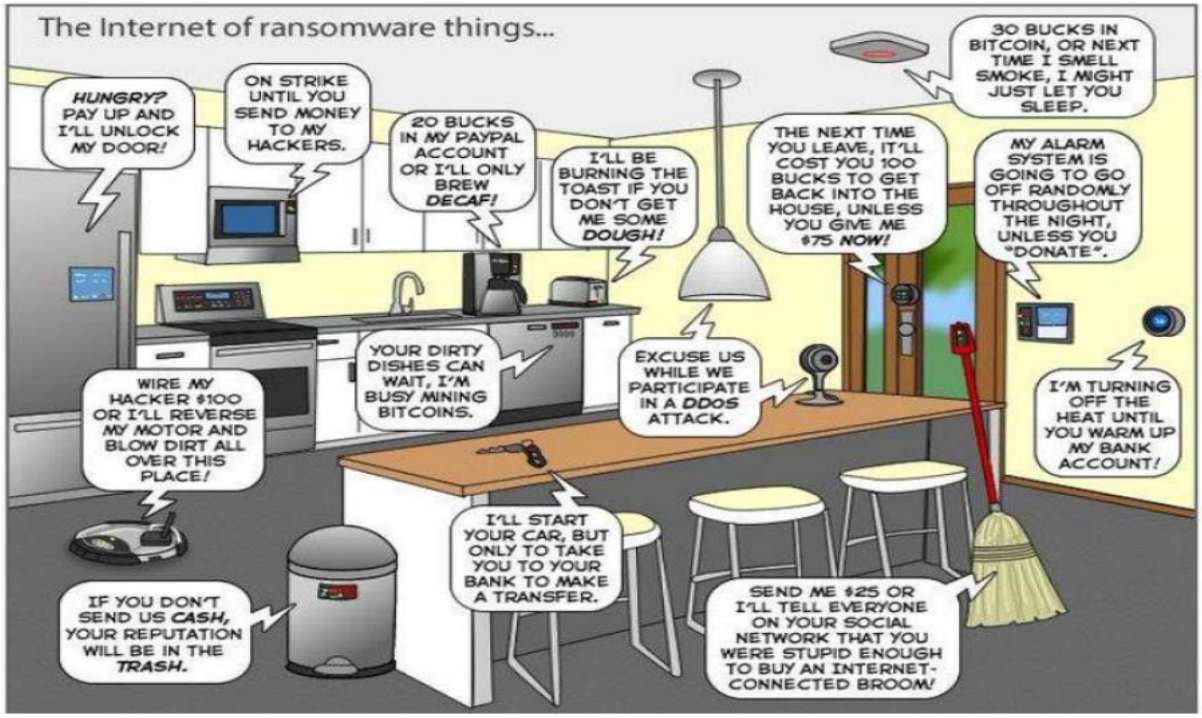
La ricerca, che ha coinvolto 11 Paesi per un totale di 2.647 responsabili security e IT intervistati. Il numero medio annuo di security breach per azienda è aumentato da 50 a 62 (+20% in Italia contro un +11% a livello

MENU | CERCA la Repubblica

HOME MACROECONOMIA FINANZA LAVORO DIRITTI E CONSUMI AFFARI&FINANZA OSSERVA ITALIA

Cybersicurezza , il mercato in Italia vale 1,5 miliardi (ma è insufficiente)

Indagine della società di consulenza EY: solo il 45 per cento delle imprese ha investito contro gli attacchi informatici. Nel mondo verranno creati nel settore due milioni di posti lavoro in cinque anni



Scenario di CASA

Scenario personale

CONSIGLIO NAZIONALE INGEGNERI | C3i COMITATO ITALIANO INGEGNERIA INFORMAZIONE

Lavora in modalità sicura anche da casa

Le 10 Regole da seguire per una maggiore Cyber Sicurezza dei propri dati

01 BACKUP
Effettua giornalmente i Backup dei tuoi dati su dispositivi esterni (es. HD, Flashdrive, etc)

02 PASSWORD
Utilizza password robuste (almeno 8 caratteri e con caratteri speciali). In particolare quando condividi i dati all'esterno

03 ANTIVIRUS
Installa sistemi di Antivirus sia sul tuo computer che sul tuo smartphone e tienili costantemente aggiornati

04 ALLEGATI
Fai attenzione ad email ingannevoli e non aprire allegati. Nel caso cancella la email e notifica l'accaduto al responsabile della sicurezza

05 SOCIAL ENGINEERING
Fai attenzione ad attacchi di ingegneria sociale. Non condividere informazioni sensibili con terzi non autorizzati

06 VPN
Usa sempre connessioni sicure (Virtual Private Network) tra il tuo PC ed il server contenente i dati sensibili

07 CONDIVISIONE
Non usare strumenti di condivisione dati pubblici (es. Wetransfer) ma cloud privati (es. Google Cloud, Azure, DropBox), proteggendo i dati con password robuste

08 CRITTOGRAFIA
Utilizza strumenti di crittografia della posta elettronica, in caso di condivisione di dati sensibili

09 PROCEDURE
Implementa e segui le procedure di sicurezza, in termini di SW da utilizzare e azioni da intraprendere in caso di data breach (perdita dati)

10 ACCESSI
Implementa e assicurati di tracciare gli accessi (Log-In e Log-Out) degli utenti ai sistemi e postazioni di lavoro

GdL Cyber Security

CONSIGLIO NAZIONALE INGEGNERI | C3i COMITATO ITALIANO INGEGNERIA INFORMAZIONE

01 BACKUP
Effettua giornalmente i Backup dei tuoi dati su dispositivi esterni (es. HD, Flashdrive, etc)

Va effettuato almeno 1 volta a settimana in maniera incrementale e una volta a mese full. Possibilmente su supporti esterni o cloud

02 PASSWORD
Utilizza password robuste (almeno 8 caratteri e con caratteri speciali). In particolare quando condividi i dati all'esterno

Cambiarla almeno ogni 90 gg. In alcuni casi prevedere dei sistemi di doppia autenticazione come impronta digitale o 2FA

03 ANTIVIRUS
Installa sistemi di Antivirus sia sul tuo computer che sul tuo smartphone e tienili costantemente aggiornati

Va aggiornato almeno ogni settimana. Meglio ancora se combinato con un Firewall dello studio/azienda o previsto dal contratto dell'operatore telefonico

04 ALLEGATI
Fai attenzione ad email ingannevoli e non aprire allegati. Nel caso cancella la email e notifica l'accaduto al responsabile della sicurezza

Generalmente è consigliabile fare analizzare gli allegati all'antivirus prima di aprirlo. Nei casi più complessi si possono usare delle Sandbox cosi da comprenderne/mitigarne il rischio

Prendere tempo, fare molte domande al richiedente sulla sua identità e non divulgare informazioni sensibili. In casi eclatanti fare denuncia alla Polizia Postale

Va utilizzata principalmente quando si lavora in modalità smartworking o si vuole accedere al proprio Server in modalità sicura

Nel caso di condivisione di file nel cloud è sempre buona norma proteggerli con una password (ie ZIP file) o se possibile crittografarli

Quando si vuole condividere un informazioni altamente sensibile (es. un progetto di un cliente). In questo caso usare almeno una crittografia a 128 bit

09 **PROCEDURE**
Implementa e segui le procedure di sicurezza, in termini di SW da utilizzare e azioni da intraprendere in caso di data breach (perdita dati)

Vanno revisionate almeno una volta l'anno. Tramite dei piani di Audit ed un piano di Remediation

10 **ACCESSI**
Implementa e assicurati di tracciare gli accessi (Log-In e Log-Out) degli utenti ai sistemi e postazioni di lavoro

Configurando opportuni sistemi di protezione perimetrale come Firewall o IDS. Tracciare le operazioni effettuate dagli utenti tramite i LOG di accesso o di eventi di sistema.

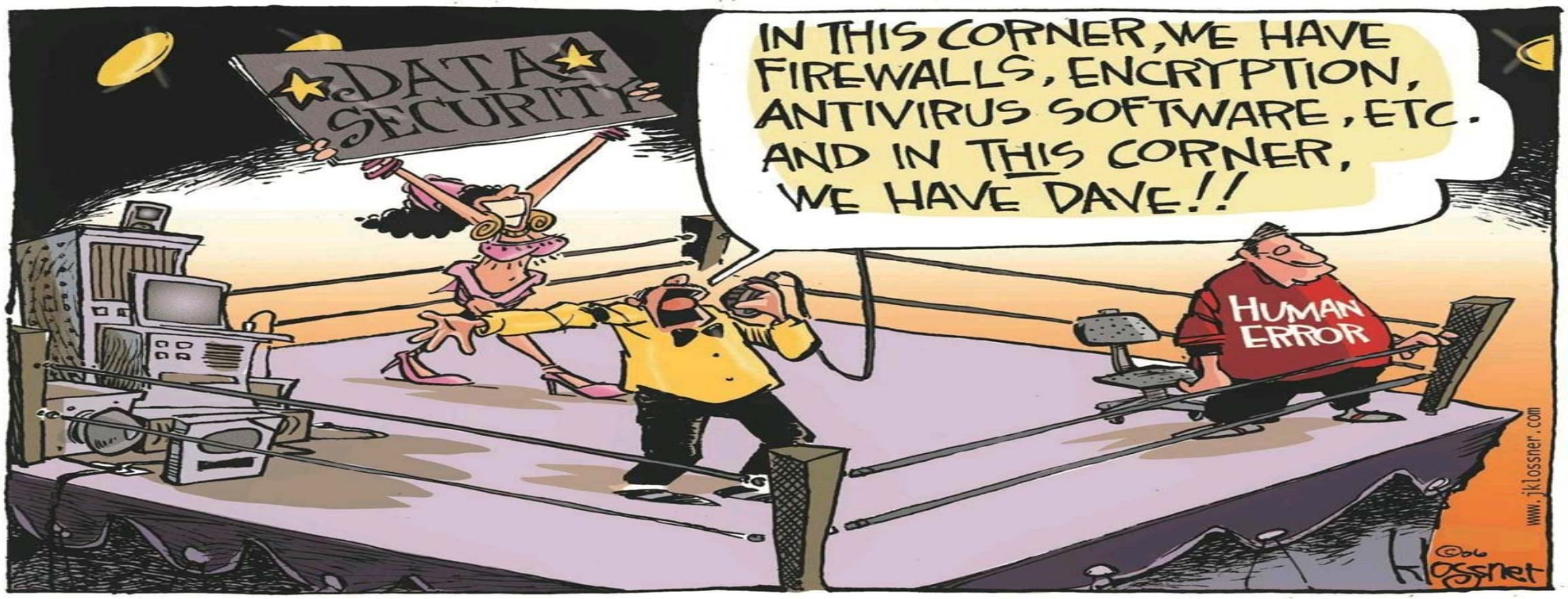
CONSIGLIO NAZIONALE INGEGNERI | C3i COMITATO ITALIANO INGEGNERIA INFORMAZIONE

Esistono diversi rischi e minacce nel mondo dell'IT, ognuna della quali ha un impatto sull'operatività e sui dati diversa.

Oltre ai 10 elementi e regole da seguire per un corretto uso in sicurezza dei nostri dati, ne **esiste una 11 esima, legata alla possibilità di sottoscrivere una contratto assicurativo in caso di data breach o attacco informatico**. Dove però la responsabilità primaria ricade sempre nel Titolare del dato stesso.

Non esiste un livello di sicurezza massimo, ma il tutto si basa sulla consapevolezza del singolo rispetto alla percezione del rischio.

CONSIGLIO NAZIONALE INGEGNERI | C3i COMITATO ITALIANO INGEGNERIA INFORMAZIONE



«Security is a process, not a product»
Bruce Schneier

GdL Cyber Security