SicurAzienda BLOG

SEGRETERIA@SICURAZIENDA.COM
WWW.SICURAZIENDA.COM

20 DICEMBRE 2023

Cyber security: le aziende sono davvero protette?
L'importanza d'investire nella difesa digitale

L'era digitale ha portato con sé una crescente dipendenza dalle tecnologie informatiche, sia per privati che per aziende. La **cyber security** è diventata un **argomento di vitale importanza** in un mondo sempre più interconnesso, specialmente con lo sviluppo tecnologico degli ultimi anni, che ha favorito un'**evoluzione delle minacce cibernetiche senza precedenti**, con il conseguente aumento dei **rischi di furto di dati sensibili, sabotaggio di operazioni aziendali e crollo della fiducia dei clienti**.

Questa **crescente digitalizzazione**, unita alla **fisiologica dipendenza dalla tecnologia**, impongono l'**adozione di coperture assicurative e strumenti di protezione dalle minacce** in grado di minimizzare i rischi societari.

Nonostante il contesto indichi chiaramente la strada da percorrere, **molte aziende italiane rimangono indietro nell'implementazione e nell'avanzamento della protezione** da cyber attacchi. I motivi? Sia per **ragioni di budget che per errata valutazione dei rischi**, diverse imprese **sottovalutano spesso l'urgenza di investire nella sicurezza** cibernetica.

Per comprendere l'**entità della minaccia**, possiamo fare riferimento ai dati forniti dal **rapporto annuale sull'Internet Crime dell'FBI,** che evidenzia danni per **6,9 miliardi di dollari nel 2021** causati da reati informatici.
Tali cifre rappresentano un campanello d'allarme, indicando l'**ampia portata delle minacce informatiche**.

Altro dato rilevante è legato agli attacchi di phishing. **Nel 2022 sono stati oltre 500 milioni, più del doppio di tutti gli attacchi registrati del 2021**.

Ma **cosa possono fare nel concreto le imprese per migliorare** da subito **la barriera di protezione** di queste minacce?

Uno degli strumenti più efficaci per proteggersi da attacchi automatizzati, che costituiscono la grande parte delle minacce informatiche, è implementare misure di **autenticazione multifattoriale** (Multi-Factor Authentication).

La **MFA**, se adeguatamente implementata, può bloccare il **99,9% degli attacchi automatizzati,** inclusi il **phishing**, gli **attacchi brute force** e i **keylogger**.

DIFESA DIGITALE: COSA POSSONO FARE NEL CONCRETO LE IMPRESE

Implementare misure di autenticazione multifattore

Effettuare un corretto Vulnerability Assesment

Investire nella formazione dei dipendenti

Il **secondo aspetto critico** che emerge dal nostro dialogo quotidiano con le aziende è la **mancanza di un corretto Vulnerability Assessment**.
Questo processo **comporta l'identificazione e la correzione delle debolezze presenti nella rete** e nei sistemi aziendali.
L'identificazione delle vulnerabilità è un passo essenziale per garantire che l'azienda sia protetta contro possibili attacchi informatici.

Terzo elemento nel quale le aziende risultano carenti è dato dalla **scarsa formazione dei dipendenti**, un aspetto spesso trascurato ma **cruciale nella prevenzione dei rischi informatici**.
Gli **esseri umani sono** spesso **il punto debole nella catena di sicurezza**, poiché gli **attacchi di phishing** e le **minacce di social engineering** dipendono in larga parte dalla **capacità di manipolazione delle persone**.
Pertanto, è fondamentale **preparare adeguatamente e regolarmente i dipendenti**, sviluppando e consolidando la loro **capacità di riconoscimento delle minacce**, imparando a **rispondere in modo adeguato alle diverse situazioni**.

Proprio per via della rapida evoluzione delle minacce cibernetiche, **l'istruzione deve essere continua** e tenere il passo con le nuove minacce. **Un dipendente ben addestrato può decisamente essere l'elemento che fa la differenza tra un attacco di successo e un fallimento.**

ACN E GARANTE: CONSERVAZIONE DELLE PASSWORD

Le ricerche continuano a confermare come la **cattiva abitudine di creare password facili** per diversi **servizi online** sia alla base di compromissioni che portano alla **violazione** di dati personali.

Nella maggior parte dei casi, gli **attacchi** sono indirizzati a colpire **siti di intrattenimento** (35,6%), **social** (21,9%) e **e-commerce** (21,2%); mentre solo 1,3% raggiunge i **servizi finanziari**, prova che banche e istituti di credito sono tra **i più attenti** nella salvaguardia dei profili dei propri utenti.

ACN (Agenzia per la Cybersicurezza Nazionale) e **Garante privacy** hanno così deciso di mettere a punto delle **linee guida** utili ai Titolari del trattamento per la corretta conservazione delle password, con l'obiettivo di **fornire indicazioni sulle modalità ad oggi più sicure** (hashing, crittografia e algoritmi) **da implementare sui sistemi informatici utilizzati**.
Il **target di riferimento** sono le **pubbliche amministrazioni** e i fornitori di **servizi "critici"** quali **telefonia, strutture sanitarie, gestori di PEC e mail, studi legali**.
Ovviamente, le indicazioni possono essere uno spunto per realtà di ogni tipo e dimensione.

Se volete approfondire il tema, a questo link
- Garante privacy e ACN insieme per un ambiente digitale più sicuro... – **potete consultare le linee guida**.