3 crimini informatici che colpiscono le aziende

Relatore: Marco Alvise De Stefani

martedì 10 ottobre 2017, ore 14:00

FP1640985001
#Sharing3FVG

Webinar realizzato da IALFVG e parte degli 80 di #Sharing3FVG, progetto cofinanziato dal Fondo Sociale Europeo nell'ambito del Programma Operativo Regionale 2014/2020

Link alla presentazione

Al seguente link è possibile visualizzare la presentazione online utilizzata durante il webinar

https://prezi.com/r-bfaf-brmjf/sharing3fvg/

Pillole di sicurezza

- **Professionalità degli operatori**
  Scegliere fornitori che siano specializzati e competenti, evitare tuttologi.

- **Reparto IT interno**
  Se è necessario un team interno, che sia formato da personale competente e non da dipendenti con altri ruoli in azienda e che svolgono anche i ruoli IT solo perché sono "smanettoni".

- **Security Assessment**
  Prima di iniziare a correre verso un obiettivo, bisogna fermarsi e capire che strada percorrere.
  Il Security Assessment aiuta l'azienda a capire quali sono i suoi asset e come proteggerli.

Pillole di sicurezza

- **Crescita costante**
  L'infrastruttura deve crescere assieme all'azienda.
  Se l'azienda cresce troppo velocemente bisogna sapersi fermare e ristrutturare.

- **Progettazione**
  È importante avere una visione d'insieme e un progetto a lungo termine da seguire.

- **Strumenti giusti**
  Implementare e scegliere gli strumenti adatti all'azienda senza farsi condizionare dalle mode.
  Valutare anche i costi di gestione e implementazione.

Pillole di sicurezza

- **Formazione**
  Formazione (continua!) di tutto il personale per l'utilizzo consapevole dei dispositivi informatici e dei servizi digitali.
  Formazione speciale del personale IT per fornirgli gli strumenti e le competenze per realizzare la mission aziendale.

- **Policy aziendali**
  Regole chiare sull'utilizzo degli strumenti aziendali.

- **GDPR**
  La General Data Protection Regulation è un trampolino di lancio, non un obbligo inutile.
  È un'occasione per le aziende per comprendere il valore dei propri dati e ristrutturarsi.

Pillole di sicurezza

- **Infrastruttura resiliente**
  Il costo di sistemi di backup e di un'infrastruttura resiliente sembra elevato? Va prima quantificato il costo di un'ora o un giorno di blocco del sistema informatico aziendale e poi fatta una valutazione costi/benefici.

- **Monitoraggio**
  Fondamentale per potersi accorgere degli incidenti informatici, dei comportamenti illeciti interni all'azienda, di attacchi dall'esterno, ecc.
  La maggior parte delle aziende subisce furto di know how senza rendersene conto.

- **Test**
  Test casuali di phishing e ingegneria sociali sui dipendenti e collaboratori, purché siano motivo di crescita e non di punizione.

Pillole di sicurezza

- **Password**
  Password diverse per ciascun servizio e cambiate regolarmente.
  Meglio preferire frasi lunghe con qualche maiuscola e numeri piuttosto che brevi accozzaglie di lettere e simboli difficili da ricordare.

- **Utilizzo promiscuo dei dispositivi e BYOD**
  Sui dispositivi personali c'è un'attenzione inferiore rispetto a quelli lavorativi, si installano spesso software piratati che possono contenere malware, si visitano siti più a rischio, aumentando la possibilità di esfiltrazione di dati aziendali.

- **Cifratura**
  È utile per proteggere i propri dati e quelli dei clienti.

- **Social**
  Essere presenti come azienda su Internet è fondamentale.
  Assicurarsi che anche i dipendenti siano in linea con lo spirito aziendale.

GRAZIE!

destefani@legaleye.it