UNINDUSTRIA

UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE

ROMA • FROSINONE • LATINA • RIETI • VITERBO

21 GIUGNO 2021

UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

La Trasformazione digitale a portata di Impresa

DIGITAL INNOVATION SHORTCUTS

Business Security

Quanto sono consapevoli i tuoi colleghi dei rischi cybersecurity in azienda?

Cyber Security Awareness

Annamaria Benedetti
TIM

Gaetano Mungari
CNPADC

La centralità della persona nella cybersecurity

Human Risk

Il cyber spazio in cui ci muoviamo ogni giorno è un complesso ecosistema in continua evoluzione ed esposto a minacce in grado di sfruttare le «falle» nei processi e nei comportamenti delle persone, soprattutto attraverso tecniche di social engineering.

La resilienza (o la fragilità) di un sistema di cyber security è fortemente determinata dal fattore umano: occorre investire sulla persona!

La centralità della persona nella cybersecurity

Human Risk

In June 2017, A.P. Moller – Maersk fell victim to a major cyber-attack caused by the NotPetya malware, which also affected many organisations globally. As a result, Maersk's operations in transport and logistics businesses were disrupted, leading to unwarranted impact.

The attack was reportedly created huge problems to the world's biggest carrier of seaborne freight which transports about 15 per cent of global trade by containers. In particular, Maersk's container ships stood still at sea and its 76 port terminals around the world ground to a halt. The recovery was fast, but within a brief period the organisation suffered financial losses up to USD300m covering, among other things, loss of revenue, IT restoration costs and extraordinary costs related to operations.

All began when an employee in Ukraine responded to an email which featuring the NotPetya Malware. The system affected and therefore operations practically had to be on hold until system's restoration.

Un lavoratore non opportunamente istruito potrebbe non essere in grado di riconoscere un tentativo di attacco cyber e, inconsapevolmente, favorire uno dei primi passi della "**cyber kill chain**".

Lavorare sulla percezione del rischio

Human Risk

*«La percezione del rischio è un processo cognitivo coinvolto in diverse attività quotidiane e che orienta i comportamenti delle persone di fronte a decisioni che coinvolgono dei rischi potenziali.»**

La prevenzione del rischio cyber inizia anche da **un'efficace e continua formazione e sensibilizzazione** del personale aziendale sui rischi di sicurezza informatica.

+ CONOSCENZA = + CONSAPEVOLEZZA

* Pubblicazione web sulla percezione del rischio da parte dei membri del gruppo di ricerca -Dipartimento di Psicologia dello Sviluppo e della Socializzazione - Università degli Studi di Padova

La soluzione di Security Awareness&Traning di TIM

- **Identificare il livello di human risk dell'azienda**, attraverso attività di phishing/smishing attack simulation per definire una **roadmap efficace** di formazione dei dipendenti

- **Formare e sensibilizzare alla gestione del rischio i dipendenti,** in linea con le esigenze aziendali, combinando la teoria con demo live e casi reali di hacking

- **Rappresentare e verificare** i risultati

Benefici

Quali sono gli impatti nel business?

- Minimizzare il livello di rischio che insiste sulle persone
- Rafforzare la cyber security posture aziendale

Cosa cambia nel modo di lavorare

La sicurezza in azienda

Colleghi più responsabili in grado di:

- **gestire l'incertezza,** imparando a cogliere i cambiamenti di scenari (le minacce si presentano in diverse forme!)

- **percepire il rischio cibernetico**, diventando consapevoli delle conseguenze derivanti dalle diverse tecniche di attacco e dal proprio comportamento

UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO