MARSH RISK CONSULTING

La consapevolezza come primo fattore di difesa dal rischio cyber

1 luglio 2020

Gianvincenzo Fedele
Marsh Risk Conslulting

MARSH

Agenda

Sezione #1: Benefici e rischi del mondo digitale

Sezione #2: Il rischio informatico

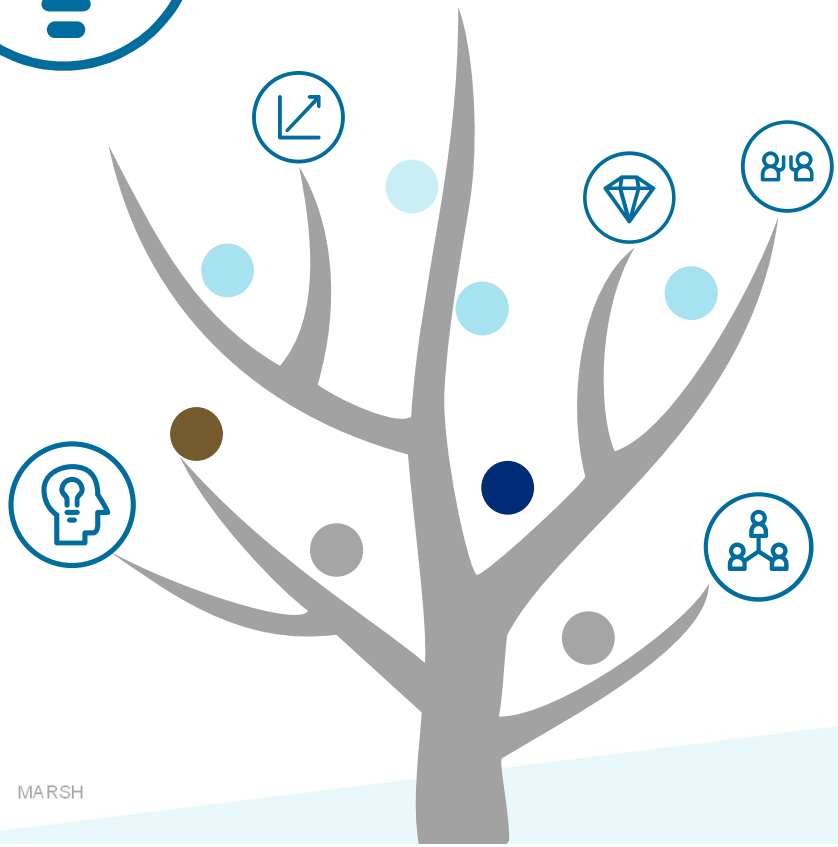
Sezione #3: Sviluppare la consapevolezza del rischio

Sezione 1

Benefici e rischi del mondo digitale

Benefici e rischi del mondo digitale
Un mondo di opportunità

Il processo di digitalizzazione che ha coinvolto la società in cui viviamo ha permesso di raggiungere benefici prima impensabili per individui ed organizzazioni



Decision-making migliorato
Raccogliendo, analizzando e presentando i dati provenienti dal mondo digitale

Riduzione delle distanze fisiche
Attraverso l'utilizzo di strumenti come i social network o piattaforme di messaggistica

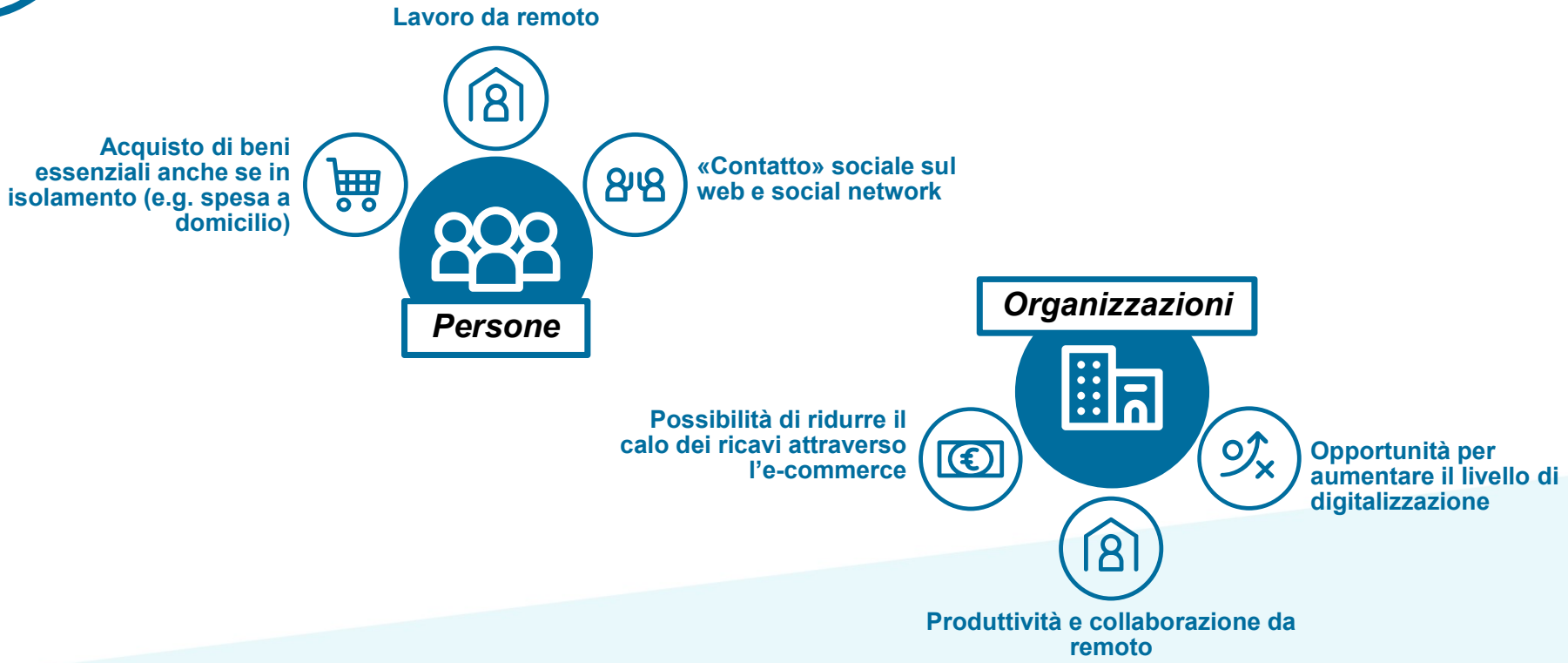
Aumento di efficienza e produttività
Attraverso l'adozione di tecnologie a supporto della produzione e per ridurre task ripetitivi per l'uomo

Miglioramento nella comunicazione e collaborazione
Utilizzo di strumenti ad-hoc che facilitano la condivisione di informazioni anche da remoto

Maggiori incentivi per l'innovazione
Attraverso la necessità di stare al passo con i tempi con le nuove tendenze digitali

Benefici e rischi del mondo digitale
Un mondo di opportunità: un caso concreto

Che supporto hanno dato le tecnologie digitali a persone ed organizzazioni nell'affrontare il periodo di lock-down a seguito della diffusione del Covid-19?



Benefici e rischi del mondo digitale
Un mondo di opportunità… e di rischi

Trend del mondo digitale

Uso estensivo dei sistemi IT
Crescente dipendenza dei processi di business dalla disponibilità di piattaforme software critiche

Complessità della tecnologia
La tecnologia diventa sempre più sofisticata, pervasive ed integrata

Condivisione e scambio di dati
Aumento delle interconnessioni e della velocità e del volume dei dati scambiati in rete

Aumento dell'attività su internet
L'aumento della presenza individuale su internet aumenta il livello di esposizione dei nostri dati personali

Utilizzo di social network
Se usati in modo errato, i social network rappresentano una pericolosa bacheca digitale della nostra vita sociale e lavorativa

Rischi connessi al mondo digitale

1. Aumento delle superfici di attacco
2. Incremento degli impatti derivanti da attacchi informatici
3. Maggiore complessità dei sistemi di protezione

Tutte le tracce che lasciamo delle nostra vita personale su internet sono alla portata dei malintenzionati e possono essere usate contro di noi!

Benefici e rischi del mondo digitale
Siamo vulnerabili ai rischi digitali allo stesso modo dei rischi fisici (1/2)

È corretto considerare e gestire i rischi connessi al mondo fisico ed i rischi connessi al mondo digitale in modo differente?

Calamità naturali

Furti

Guasti

Incidenti stradali

Adescamento

Truffe

Sottrazione di informazioni

RISCHI DEL MONDO FISICO

VS

Clonazione del profilo social

Furto dell'identità digitale

Intrusione nei device

Violazione della privacy

Truffe digitali

Furto delle credenziali

Sottrazione di informazioni

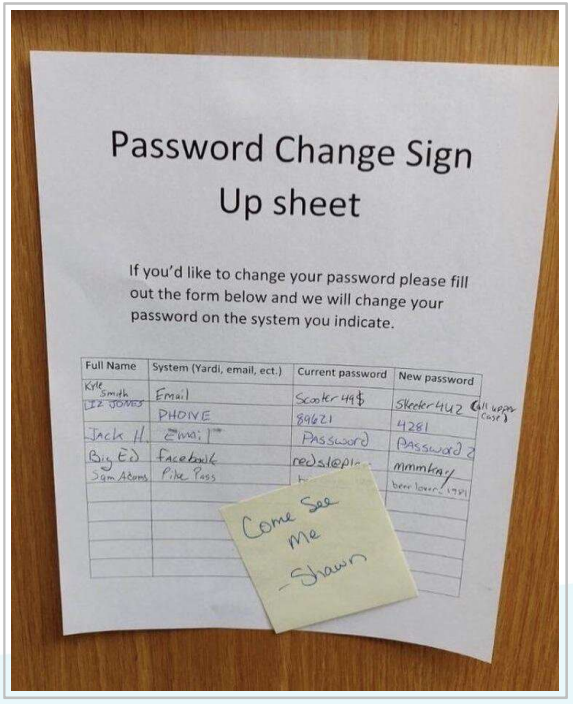
RISCHI DEL MONDO DIGITALE

Benefici e rischi del mondo digitale

Siamo vulnerabili ai rischi digitali allo stesso modo dei rischi fisici (2/2)

Come proteggeresti l'ingresso di casa tua?
Lasceresti mai le chiavi incustodite?

Fonte: The Cyber Security Hub



Fonte: The Cyber Security Hub

Sezione 2

Il rischio informatico

Il rischio informatico
Un rischio reale: casi recenti di cyber-attacchi

La situazione di emergenza apportata dal Covid-19 e l'attivazione massiva di infrastrutture per il lavoro da remoto, ha aumentato la vulnerabilità ad attacchi cyber

ATTACCO INFORMATICO

Geox sotto cyber-attacco: azienda colpita con richiesta di riscatto

di Redazione Economia | 16 giu 2020

MONDO

Coronavirus, Nyt: "Fbi e Sicurezza Nazionale Usa in allarme per cyber-attacchi cinesi ai centri di ricerca sul vaccino anti-Covid"

Attacco informatico contro la compagnia aerea EasyJet, interessati anche 480mila svizzeri

In un numero limitato di casi i criminali informatici hanno avuto accesso ai dati delle carte di credito dei clienti

Home . Magazine . Cybernews .

Coronavirus, Leonardo rileva 230mila cyber attacchi nel mondo, 6% verso Italia

CYBERNEWS

Mi piace 0 Condividi Tweet Share

Allarme ransomware su Enel e Honda, reti interne bloccate e disservizi

Il rischio informatico
Le cause dei cyber-attacchi

Le cause degli attacchi cyber possono ricondursi principalmente a due grandi macro-categorie di fattori che spesso vengono combinati per il buon esito dell'attacco

Fattori umani

- Studio individuale dei comportamenti digitali e fisici della persona allo scopo di ottenere informazioni utili
- Tali informazioni sono utilizzate per eseguire attacchi informatici alle aziende, frodi o furti di identità

La prima minaccia per l'azienda in cui lavoriamo potremmo essere noi ed il nostro comportamento!

Fattori tecnici

- Messa a punto di strumenti di hacking per introdursi nelle reti dell'azienda
- Tali strumenti sfruttano delle vulnerabilità sia tecniche che organizzative per generare effetti devastanti

Le tecniche di hacking trovano terreno fertile in organizzazioni con un approccio non strutturato alla sicurezza delle informazioni!

La prima linea di difesa è lo sviluppo della consapevolezza del rischio informatico sia sulla dimensione individuale che su quella organizzativa

Il rischio informatico
Le cause dei cyber-attacchi: Social Engineering

È più facile spingere una persona a rivelare le proprie password rispetto all'ottenere tali informazioni mediante tecniche da hacker…

Social Engineering

L'atto di studiare il comportamento individuale e manipolare le persone affinché compiano azioni specifiche a vantaggio dell'attaccante*

Si basa sulla tesi che vede il fattore umano essere l'anello più debole della catena della sicurezza informatica

Metodi di attacco

- Pretexting
- Phishing
- Spear-Phishing
- Baiting
- Vishing

Tecniche Psicologiche

- Autorevolezza
- Senso di colpa
- Panico
- Ignoranza

* Fonte: Avast

Sezione 3

Sviluppare la consapevolezza del rischio

Sviluppare la consapevolezza del rischio
Le dimensioni della consapevolezza del rischio in azienda

Come è possibile sviluppare efficacemente la consapevolezza del rischio cyber in azienda e quali sono gli strumenti che possono essere utili allo scopo?

Dimensione Organizzativa

Conoscenza dell'esposizione alle perdite derivanti da minacce di natura informatica dal punto di vista dell' organizzazione nel suo complesso.

Fornisce lo stimolo a tutti gli aspetti tecnologici, organizzativi e di processo per la gestione dei rischi cyber.

Cyber Risk Quantification

Analizzare e presentare il rischio cyber dal punto di vista delle perdite economiche ad esso associate

Dimensione Individuale

Conoscenza e capacità di gestione delle situazioni anomale connesse al mondo digitale che possono interessare il singolo dipendente.

Ognuno gioca il proprio ruolo nel costruire la sicurezza dell'organizzazione!

Information Security Awareness Program

Organizzare un programma di training per i dipendenti composto da tecniche, canali e strumenti differenziati

Sviluppare la consapevolezza del rischio
Cyber Risk Quantification

Evolvere l'analisi e la comunicazione del rischio cyber è fondamentale per sviluppare la consapevolezza dell'organizzazione in merito alla propria esposizione alle minacce

Valutazione qualitativa dei rischi cyber

Risk Rating

- Rischio alto
- Rischio medio
- Rischio basso

Vulnerabile al «*bias cognitivo*»
Risk model poco strutturati
Assunzioni poco definite e non tracciate

Cyber Risk Quantification

Risk Exposure

- € 1.230.000 ogni 4 anni
- € 700.000 ogni 4 anni

Analisi di scenario effettuata attraverso stime e conseguente modellizzazione statistica dei fattori di rischio

Principali benefici

01 Linguaggio di comunicazione universale

02 Supporto alla definizione delle strategie di business

03 Prioritizzazione degli investimenti

04 Compliance a requisiti normativi

05 Definizione dei livelli di Risk Appetite

06 Ottimizzazione di un'eventuale copertura assicurativa

Sviluppare la consapevolezza del rischio
Information Security Awareness Program

Le azioni implementate dall'azienda in termini organizzativi e tecnologici spesso non bastano se i malintenzionati prendono di mira le singole persone

Sessioni di formazione

Lezioni in aula e/o webinar per apprendere concetti di base sulla sicurezza informativa e sulle relative procedure organizzative

Simulazioni

Simulazioni di minacce reali (e.g. campagne di phishing) per testare il comportamento dei dipendenti

Campagne informative

Predisposizione di materiale cartaceo da affliggere nei locali e/o «pillole informative» da inviare periodicamente ai PC dei dipendenti

L'efficacia del programma è garantita dalla possibilità di apprendimento, test e aggiornamento messa a disposizione dei dipendenti

Contatti

Gianvincenzo Fedele
Responsabile Area Business Resilience
Marsh Risk Consulting

Gianvincenzo.Fedele@marsh.com

Grazie per l’attenzione

MARSH RISK CONSULTING

Il presente documento ha un mero scopo informativo e contiene informazioni riservate di proprietà di Marsh Risk Consulting Services S.r.l. (“MRC”) che non possono essere condivise con terzi, senza previo consenso scritto di MRC.
Le informazioni contenute nel presente documento provengono da fonti ritenute affidabili, tuttavia MRC non ne garantisce l’accuratezza. MRC non si assume, inoltre, alcun obbligo di aggiornamento del documento e declina ogni responsabilità nei confronti dell’azienda o di terzi che ne utilizzino il contenuto a qualsiasi titolo. Qualsiasi dichiarazione relativa a questioni attuariali, fiscali, contabili o legali si basa esclusivamente sulla esperienza di MRC quale consulente in materia di rischi e non deve essere considerata, in alcun modo, come parere di natura attuariale, contabile, fiscale o legale, per i quali si consiglia, invece, di rivolgersi ai propri consulenti. Qualsiasi analisi e informazione resa con il presente documento è soggetta a incertezza intrinseca e il contenuto del presente documento potrebbe risultare compromesso nel caso in cui le presupposizioni, condizioni, informazioni o fattori contenuti nello stesso fossero inaccurati o incompleti o dovessero subire modifiche. Sebbene MRC possa fornire consigli e raccomandazioni, tutte le decisioni sulle misure da adottare in relazione allo specifico contesto sono di responsabilità dell’azienda, che decide cosa ritiene appropriato per la propria realtà.
Marsh Risk Consulting Services fa parte del Gruppo Marsh & McLennan Companies.

Copyright ©2020 Marsh S.p.A. Tutti I diritti sono riservati.