IL DIGITALE
LA CHIAVE DEL BUSINESS

Progetto promosso dal Sistema camerale dell'Emilia-Romagna per favorire la diffusione della conoscenza quale strumento di sviluppo del business, articolato in seminari di sensibilizzazione rivolti alle imprese (www.ucer.camcom.it)

Unioncamere Emilia-Romagna

Camera di Commercio Forlì-Cesena

Camera di Commercio Modena

Camera di Commercio Parma

Camera di Commercio Ravenna

Camera di Commercio Rimini

In collaborazione con Unioncamere

Il digitale: la chiave del business

SOCIAL MEDIA COME RENDERE PIÙ SOCIAL L'IMPRESA	12 MAGGIO '16 ORE 14.00/18.00	CAMERA DI COMMERCIO DI RIMINI
E-COMMERCE UN'OPPORTUNITÀ DI SVILUPPO	12 APRILE '16 ORE 14.00/18.00	CAMERA DI COMMERCIO DI RAVENNA
CLOUD COMPUTING ISTRUZIONI PER L'USO	5 MAGGIO '16 ORE 14.00/18.00	CAMERA DI COMMERCIO DI RIMINI
SCM E CRM LEVE PER LA COMPETITIVITÀ	5 APRILE '16 ORE 14.00/18.00	CAMERA DI COMMERCIO DI FORLÌ
	7 APRILE '16 ORE 14.00/18.00	CAMERA DI COMMERCIO DI PARMA
DATA BIG AND OPEN	21 APRILE '16 ORE 9.00/13.00	CAMERA DI COMMERCIO DI MODENA
IOT INTERNET OF THINGS E INDUSTRY 4.0	19 APRILE '16 ORE 14.00/18.00	CAMERA DI COMMERCIO DI FORLÌ
	31 MARZO '16 ORE 14.00/18.00	CAMERA DI COMMERCIO DI PARMA
LA SICUREZZA NEL WEB DI COSA E PERCHÈ	7 APRILE '16 ORE 9.00/13.00	CAMERA DI COMMERCIO DI MODENA
	28 APRILE '16 ORE 14.00/18.00	CAMERA DI COMMERCIO DI RAVENNA

LA SICUREZZA NEL WEB

DI COSA E PERCHÈ

PARMA 31 MARZO 2016

Unioncamere Emilia-Romagna

Camera di Commercio Parma

In collaborazione con

Unionтrasporti

Trasporti Logistica Infrastrutture

Perché questo seminario ?

Il digitale e il web se da un lato ci offrono nuove modalità di comunicazione e di interazione non solo tra persone ma anche con le cose, generando nuove opportunità di business e modificando il nostro modo i lavorare e di vivere, dall'altro ci espone ad una serie di rischi quali la perdita o l'appropriazione indebita dei nostri "dati" siano essi personali/aziendali o di clienti e fornitori da noi raccolti o che ci sono stati affidati.

Il perimetro della rete IT aziendale si allargando perché interagiamo indipendentemente dalla nostra posizione e dal dispositivo (mobile) attraverso applicazioni in cloud.

Dobbiamo guardare però non solo all'esterno ma anche all'interno dell'azienda.

La posta in gioco è alta: ne va non solo dell'operatività di un'azienda ma anche dei suoi risultati reddituali e della sua reputazione (Digital economy si basa sulla fiducia nella sicurezza dei dati personali)

Il comportamento delle imprese non sempre è guidato da uno studio delle vulnerabilità, delle minacce e del loro impatto sul business. Spesso si reagisce a seguito di un evento andato a segno: ad esempio un attacco di un virus, la perdita del controllo sui dati di clienti e fornitori finiti in mani non autorizzate.

Obiettivi del seminario

Rispondere alle seguenti domande:

1. Quali sono i rischi a cui la mia impresa è esposta ?
2. Quali sono le tecnologie presenti in grado di mitigare il rischio senza bloccare l'operatività dell'azienda ?
3. Quale livello di investimento devo prevedere ?

Il relatore

Ing. Gianluca Golinelli

Consulente di sicurezza informatica
Esperto di informatica forense per il tribunale di Parma
Docente Ifoa

ifoa Sapere utile

Non dimenticate di darci un feedback

Questionario on-line al seguente indirizzo:

https://docs.google.com/forms/d/1t_PZEienue4UYALariu1iPceCeLBBY7fMXRwlJ46wmQ/viewform

Relatore: Ing. Gianluca Golinelli

Sommario

1. Principali vulnerabilità e minacce presenti nelle soluzioni web
2. Elementi per un'autovalutazione di vulnerabilità / rischi / impatti
3. Implicazioni organizzative e di modello di funzionamento in grado di arginare le minacce
4. Soluzioni tecnologiche disponibili, investimento economico richiesto ed il processo di introduzione raccomandato
5. Casi di studio: buone e cattive pratiche

1. Principali vulnerabilità e minacce

Delitti denunciati dalle f

dati.istat.it/Index.aspx?DataSetCode=dccv_delittips#

PayPal Facebook Twitter Libero Mail eBay YouTube LinkedIn Nessus

I.Stat versione di prova — il tuo accesso diretto alla statistica italiana

Login | English Version | FAQs e Contatti | Manuale utente | Home

Ricerca

Per Iniziare

Esplora Temi | Tabelle più richieste

Cerca nei temi — Annulla

Giustizia e sicurezza

- Censimento agricoltura 2010
- Censimento industria,istituzioni pubbliche e non profit 2011
- Censimento popolazione e abitazioni 2011

Giustizia e sicurezza

- Giustizia civile
- **Giustizia penale**
  - Numero procedimenti penali
  - Procedimenti e reati al momento della decisione del PM - adulti
  - Segnalazioni relative a persone denunciate e arrestate/fermate dalle forze di polizia
  - **Delitti denunciati dalle forze di polizia all'autorità giudiziaria**
    - Delitti in totale per tipo di delitto - livello nazionale
    - Delitti con presunti autori noti per tipo di delitto, periodo del commesso delitto - livello ripartizionale e regionale
    - Delitti in totale per tipo di delitto - livello ripartizionale, regionale e provinciale
    - Delitti in totale e con presunti autori noti per periodo del commesso delitto - livello provinciale

Delitti denunciati dalle forze di polizia all'autorità giudiziaria

Personalizza | Esportazioni | Grafici | La tua interrogazione

Territorio	Italia
Tipo dato	numero di delitti denunciati dalle forze di polizia all'autorità giudiziaria
Identità autore nota	totale
Periodo del commesso delitto	durante l'anno di riferimento

Tipo di delitto \ Anno	2006	2007	2008	2009	2010	2011	2012	2013	2014
truffe e frodi informatiche	109 059	120 710	104 174	99 366	96 442	105 692	116 767	140 614	133 261
delitti informatici	2 394	3 799	4 952	5 510	5 973	6 933	7 346	9 421	10 846
ricettazione	30 042	31 104	27 786	23 619	23 686	23 773	25 080	25 275	24 935
riciclaggio e impiego di denaro, beni o utilità di provenienza illecita	1 193	1 209	1 253	1 269	1 344	1 350	1 685	1 891	1 604
usura	353	382	375	464	374	352	405	460	405
danneggiamenti	344 253	384 529	402 163	415 391	414 923	398 521	364 435	341 152	279 277
incendi	12 659	16 716	12 662	10 921	9 622	12 980	13 170	7 388	6 855
incendi boschivi	3 688	7 049	4 499	3 734	2 770	5 870	6 105	2 035	1 775
danneggiamento seguito da incendio	10 104	11 762	10 728	9 797	9 721	10 499	11 209	9 815	8 572
normativa sugli stupefacenti	32 306	34 439	34 082	34 101	32 761	34 034	33 852	33 578	33 246
attentati	618	544	447	376	490	439	522	462	386
associazione per delinquere	1 074	1 011	871	872	744	906	943	792	986
associazione di tipo mafioso	128	140	125	131	128	93	68	75	89
contrabbando	1 150	1 096	1 062	1 132	1 067	1 034	1 284	1 254	1 231
altri delitti	363 629	388 842	415 138	420 252	409 525	403 735	410 997	459 478	439 120
totale	2 771 490	2 933 146	2 709 888	2 629 831	2 621 019	2 763 012	2 818 834	2 892 155	2 812 936

Dati estratti il 22 mar 2016, 21h18 UTC (GMT), da I.Stat

Basato sulla tecnologia datawarehouse OECD © OECD. Tutti i diritti riservati Termini e condizioni | Politica sulla privacy

Login | English Version | FAQs e Contatti | Mappa del sito | Manuale utente | Home

1. Principali vulnerabilità e minacce

I profili degli agenti di attacco

- **Virus di tipo Ransomware** : Richiesta di riscatto
- **Virus tradizionali o worms** : Danni fini a se stessi
- **Hoax**: Creare allarme, panico
- **Attacchi da Botnet**: DDos verso specifici target
- **Hackers malevoli**: Per profitto o altri benefici
- **Competitors**: Per causare danno all'azienda concorrente
- **ex-dipendenti scontenti**: Per vendetta
- **Script kiddies**: Per gioco
- **Dipendenti maldestri**: Per imperizia

1. Principali vulnerabilità e minacce

- Infezione da Virus «Crypto Ransomware», esempi di phishing:
  - E-Mail con il «contratto da firmare»
  - E-Mail con messaggio in segreteria di Whatsapp
  - E-Mail con la fattura
  - E-Mail con il link al sito del corriere per spedizione
  - E-Mail con notifica di accesso anomalo al proprio conto corrente
- Virus
- Worm

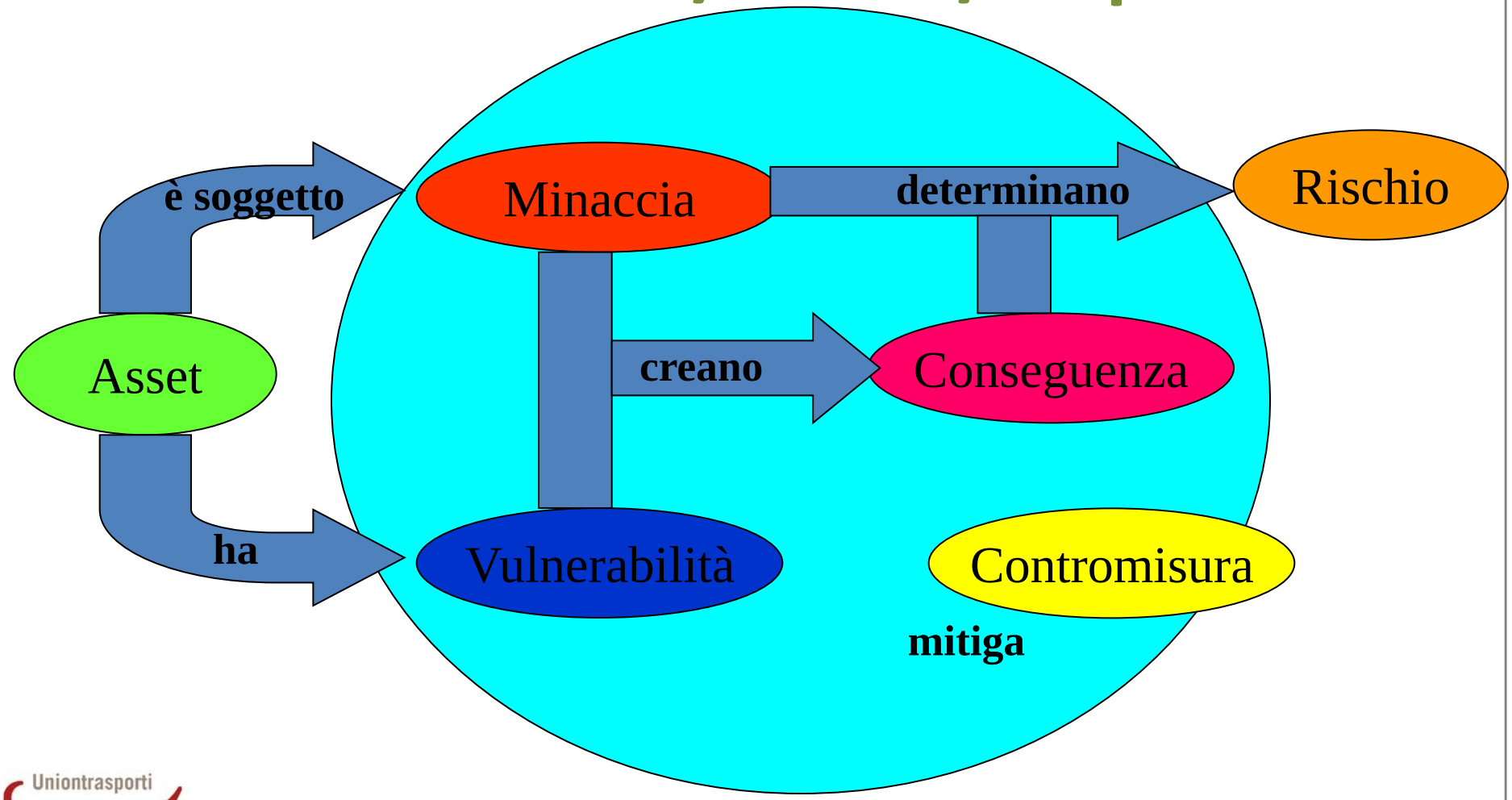
1. Principali vulnerabilità e minacce

- Furto di credenziali (credenziali carte di credito, credenziali di accesso a banche, siti social, credenziali email, etc.)
- Furto di dati (dati commerciali, amministrativi, tecnici, etc.)
- Possesso dei sistemi per ulteriori attacchi (BotNet)
- Attacco da siti Internet noti per propagare Malware

1. Principali vulnerabilità e minacce

- SPAM
- Phishing
- Drive by Download
- Social Engineering

2. Elementi per autovalutazione di vulnerabilità / rischi / impatti



2. Elementi per autovalutazione di vulnerabilità / rischi / impatti

- Impreparazione tecnica e mancanza di adeguata formazione
- Mancanza di dispositivi di protezione
- Vulnerabilità presenti nei software utilizzati
- Mancanza di Vulnerability Assessment e Penetration Tests
- Mancanza di adozione di policies tecniche, linee guida e best practices

Normative di legge

Il quadro normativo

- D. Lgs. 196/2003 – Codice in materia di protezione dei dati personali
- Provv. Garante privacy del 27/11/2008 – obblighi amministratori di sistema
- D. Lgs. 231/2001 – Codice della responsabilità degli enti – contempla reati informatici
- Nuovo Regolamento Europeo sulla tutela dei dati personali (approv. Commissione europea 15/12/2015), verrà ratificato entro il primo semestre 2016 dal consiglio europeo, 2 anni per le aziende per mettersi a norma.

3. Implicazioni organizzative e di modello di funzionamento in grado di arginare queste minacce

Linee guida per una navigazione sicura

- Aggiornamento del sistema (S.O., browser, applicazioni, etc.)
- Utilizzare soluzioni di «endpoint-security» (antivirus, crittografia, etc.)
- Porre attenzione al Phishing
- Attenzione a link interni ad una e-mail di dubbia origine

Mitigazione delle vulnerabilità

- Quali sono le componenti SW/HW più a rischio?
  - Applicazioni client
  - Applicazioni server
  - Servizi Web
  - Host e dispositivi di rete
  - WLan
  - Dispositivi mobili

4. Soluzioni tecnologiche disponibili, investimento economico richiesto ed il processo di introduzione raccomandato

➢ Strumenti di Protezione

- Sulla postazione :
  - ❑ Antivirus
- In Azienda e in Rete:
  - ❑ Sistemi di Disaster Recovery
  - ❑ Firewall,
  - ❑ Filtri Anti-spam,
  - ❑ Proxy, PenTest e VA
  - ❑ IDS/IPS

Introduzione immediata e prioritaria

Introduzione successiva raccomandata

Budget di costo

- Dispositivi di sicurezza
  - Antivirus (mediamente 5 licenze annue tra Euro 50,00 – Euro 90,00)
  - Firewall (mediamente tra Euro 1.000,00 – Euro 3000,00 + canone annuo)
  - Filtri antispam (tra Euro 900,00- Euro 2.000,00 annui x 100 caselle)
- Dispositivi e procedure per Disaster Recovery
  - NAS (Network Attached Storage) costo medio-basso e SAN (Storage Area Network) costo elevato Euro 3.000 – 5.000
- Formazione per staff tecnico
- Formazione per gli utenti
- Vulnerability Assessment e Penetration Tests (Euro 1.000 – 3.000)

5. Casi di studio

- Casi di studio:
  - Best practices e worst practices

5. Casi di studio

- Caso 1:
  - Azienda di automazioni colpita da Virus di tipo Ransomware
  - Implicazioni: perdita del know how tecnologico
  - Cause: carenze tecnologiche e procedurali

5. Casi di studio

- Caso 2:
  - Studio di commercialisti colpito da Virus di tipo Ransomware
  - Implicazioni: perdita dei dati contabili dei clienti
  - Cause: carenze tecnologiche e procedurali

5. Casi di studio

- Caso 3:
  - Azienda settore medicale succube di attacco di defacement al proprio sito web aziendale
  - Implicazioni: danno di immagine
  - Cause: carenze tecnologiche, assenza di pentest e VA

5. Casi di studio

- Caso 4:
  - Azienda settore automazioni succube di attacco di defacement al proprio sito web aziendale
  - Implicazioni: danno di immagine
  - Cause: carenze tecnologiche, assenza di PenTest e VA

5. Casi di studio

- Caso 5:
  - Azienda settore automotive succube di intrusione informatica
  - Implicazioni: danno economico
  - Cause: carenze tecnologiche, mancanza dispositivi di protezione, assenza di PenTest e VA

5. Casi di studio

- Caso 6:
  - Dipendente con PC bloccato a seguito di navigazione in siti malevoli
  - Implicazioni: danno economico
  - Cause: mancanza dispositivi di protezione, mancanza di adeguata formazione

Question time