CAMERA PENALE DI MILANO
GIAN DOMENICO PISAPIA
Aderente all'Unione delle Camere Penali Italiane

Forenser
Digital Investigations

28 ottobre 2021
Webinar

«CYBER SECURITY: RISCHI E TUTELE»
SICUREZZA AZIENDALE E TUTELA DEL KNOW HOW

Paolo Dal Checco
Consulente Informatico Forense

Chi sono

- PhD @UniTO nel gruppo di Sicurezza delle Reti e degli Elaboratori
- Passato di R&D su crittografia e sicurezza delle comunicazioni
- Piccole docenze in Master e Perfezionamento per Università degli Studi di Torino, Milano e Genova
- Consulente Informatico Forense, Perizie Informatiche per Privati, Aziende, Avvocati, Procure, Tribunali, F.F.O.O.
- Albo CTU e Periti del Tribunale di Torino, Periti ed Esperti CCIAA TO
- Tra i fondatori e nel direttivo dell'Osservatorio Nazionale d'Informatica Forense (www.onif.it)
- Socio IISFA, Tech & Law, Clusit, LAB4INT, Assob.It, AIP
- www.dalchecco.it, www.ransomware.it, www.bitcoinforensics.it, www.osintbook.it
- paolo@dalchecco.it, @forensico

Sicurezza dei sistemi informatici aziendali e domestici

- Sicurezza informatica: princìpi
  - Riservatezza
  - Integrità
  - disponibilità
- Casa o ufficio, le basi sono comuni:
  - Crittografia (PC, smartphone, cloud)
  - Software di protezione
  - Segregazione delle aree o dei ruoli (area produzione, amministrativa, progettuale, brevetti, etc…)
  - Segregazione dei privilegi (no administrator)
  - Password diverse per ogni servizio (Have I Been Pwned)
  - In casi estremi, è possibile lasciare sul proprio PC delle esche (canarytokens)

Misure di Sicurezza & Strumenti di protezione

- Un utile checklist: AGID – Misure Minime di Sicurezza per la PA
  - https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati	

https://cert-agid.gov.it/download/MM.doc

Misure di Sicurezza & Strumenti di protezione

- Strumenti essenziali (averli non vuol dire che siano usati correttamente, meglio sempre verificare):
  - Antivirus
  - Antimalware
  - Antiransomware
  - Firewall
  - Antispam
  - IDS
  - IPS

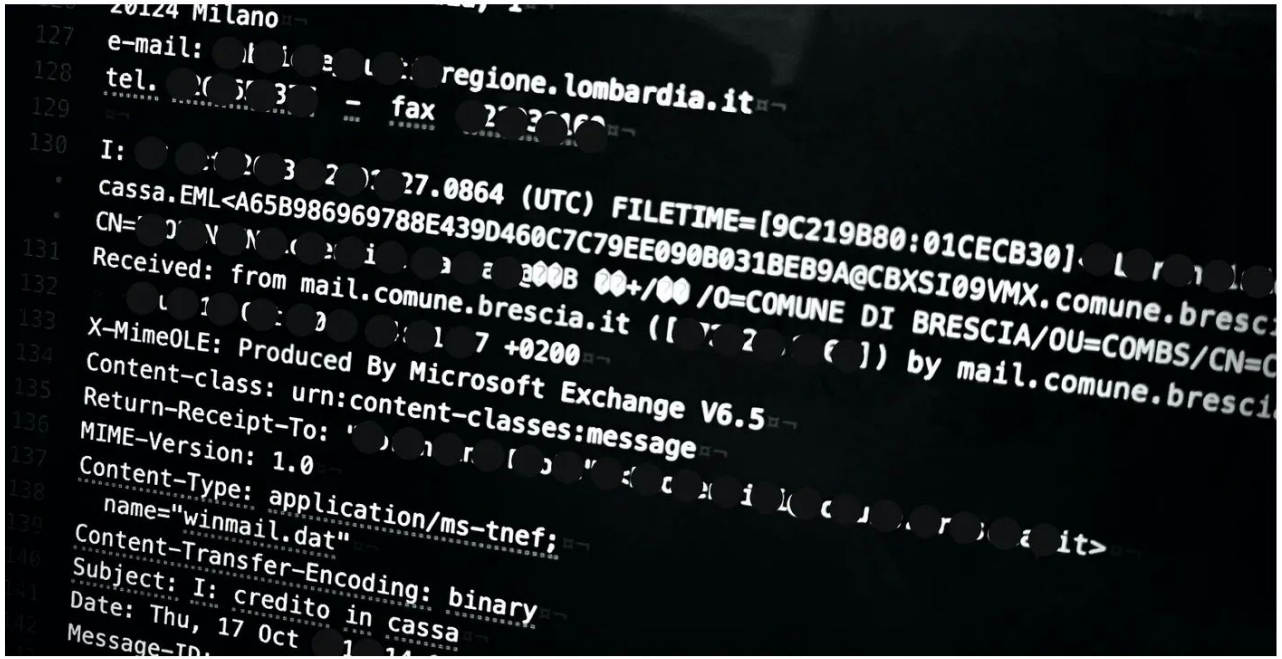
Minacce più diffuse in base all'esperienza di perito forense

- Ransomware
- Man in The Mail
- Dipendente Infedele
- Phishing per furto di credenziali
- Malware/Banking Trojan
- Account Hijack (es. Facebook page)
- Reati Informatici commessi da Dipendente a vantaggio di azienda o ente → D.Lgs 231/2001

Ransomware malware e spyware

Incubo ransomware: dal comune di Brescia a quello di Rho i dati degli italiani in vendita sul darkweb

di Roberto Pezzali - *16/04/2021 16:09* 60



Example files:

reg.lombardia credito in cassa.msg (38Kb)
ERRORE SMARTCARD.docx (285Kb)
Circolare_del_25_giugno_2014_n_21.pdf (240Kb)
00Riep.xls (39Kb)

Comune di Rho

URL: https://www.comune.rho.mi.it/it-it/home

Read more

Views: 350 | Published: 2021-04-14 16:19:42 | Updated: 2021-04-14 16:19:42

Città di Caselle Torinese

URL: http://comune.caselle-torinese.to.it/

Read more

Views: 319 | Published: 2021-04-14 16:16:20 | Updated: 2021-04-14 16:16:20

Ransomware malware e spyware

- Ransomware, all'inizio semplici programmini, ora attacchi mirati e organizzati
  - Perdita dei dati
  - Estorsione (**minaccia di divulgazione** sempre più frequente)
  - Spesso utilizzano bachi (es. Exchange con Hafnium, Fortigate, ec…)
- Malware e spyware sono simili ma con obiettivi diversi:
  - Furto d'identità
  - Ponte per ulteriori attacchi
  - Banking Trojan
  - Man in The Mail
- La difesa non è semplice
  - Comportamentale
  - Update/Patch
  - Antimalware/Firewall

Attacchi attraverso la posta elettronica

- Fenomeno più frequente: caselle di posta «bucate»
  - Per spiarne il contenuto
  - Per usarle per ulteriori attacchi
  - Per Man in The Mail (forward verso indirizzi terzi per potersi intromettere o sostituzione allegati mail)
- Soluzione: 2fa
  - SMS su numero di cellulare
  - Authentication App
  - U2F Key
- Caso frequente: Man in The Mail (posta proveniente da email simili a quelle originali)
  - Attenzione quando si risponde con il tasto «Rispondi», viene utilizzato l'indirizzo in Reply To

Gli attacchi ai dispositivi mobili

- Tipicamente no antivirus
- Android: sandbox
- iOS: sicurezza basata sul progetto e hardware (es. Secure Enclave)
- Gestione aziendale di smartphone:
  - MDM
- Protezione:
  - Antivirus/Firewall
  - Aggiornamenti e update
  - Reinstallare ogni tanto
  - Analisi forense

La vulnerabilità dei siti web

- Attacchi ai profili utente
  - Password reuse
  - Brute force
  - Misconfiguration (aree pubbliche lasciate aperte, etc….)
  - Cross authentication (autenticazione su un utente per accedere a dati di un terzo, es. referti medici, multe, etc…)
- Attacchi a database (leak, ransomware, etc…)

La vulnerabilità dei siti web

OWASP Top 10 2017		change	OWASP Top 10 2021 proposal	
A1	Injections	**as is**	A1	Injections
A2	Broken Authentication	**as is**	A2	Broken Authentication
A3	Sensitive Data Exposure	**down 1**	A3	Cross-Site Scripting (XSS)
A4	XML eXternal Entities (XXE)	**down 1 + A8**	A4	Sensitive Data Exposure
A5	Broken Access Control	**down 1**	A5	Insecure Deserialization **(merged with XXE)**
A6	Security Misconfiguration	**down 4**	A6	Broken Access Control
A7	Cross-Site Scripting (XSS)	**up 4**	A7	Insufficient Logging & Monitoring
A8	Insecure Deserialization	**up 3 + A4**	A8	**NEW:** Server Side Request Forgery (SSRF)
A9	Known Vulnerabilities	**as is**	A9	Known Vulnerabilities
A10	Insufficient Logging & Monitoring	**up 3**	A10	Security Misconfiguration

Phishing e lo Spear phishing: le tecniche d’attacco

- Come per il phishing tradizionale, ma più pericoloso perché «mirato»
- Più difficile da rilevare, anche tecnicamente
- Soluzioni tecniche:
  - DKIM, DMARK, SPF
  - Controlli euristici: mail provenienti da domini con «-it», «-com» nel dominio di secondo livello

Misure tecniche di tutela del know how e dei segreti commerciali/industriali

- Sistemi di **protezione**
  - Password (+ princìpi di sicurezza, cambio password, lunghezza, etc…)
  - Cifratura dei sistemi (dischi, smartphone, cloud)
  - Configurazione Active Directory, NAS, share, etc…
  - Firewall/NAT/Proxy/Antivirus/Etc…
- **Segmentazione della rete** e degli accessi (ACL, Access Control Lists)
- **Differenziazione dei contenuti** (tutelati vs. non tutelati)
  - Location diverse per materiale riservato
  - Logo/watermark per materiale riservato e «pubblico»
  - Notifica/banner all'utente in caso di accesso/copia/accesso di materiale riservato
- Presenza di **log storici e di sicurezza** che possano attestare gli eventi occorsi
  - Log dei NAS, posta elettronica, cloud, etc…

L’importanza del “tempo”

- Spesso avere le prove a oggi (o al momento della redazione del ricorso) non è sufficiente
  - Es. dimostrare che oggi esiste segmentazione, firewall, protezione, etc…
- È utile poter dimostrare che le configurazioni di sicurezza erano già presenti al tempo in cui si configura l’oggetto del ricorso
- Ricostruire quindi storico tramite backup/changelog/documenti/etc…
- Ove possibile, apporre data certa

Come dimostrare lo stato dei fatti

- Importante sia per i **dati** (es. server aziendale, gestionale, con know how, segreti industriali, etc…) sia per la sua **configurazione** (atta a documentare le **misure di sicurezza**)
- Copia forense (Legge 48/2008, ISO 27037, etc…)
  - **Originali inalterati**
  - **Copia identica** all'originale
  - **Copia inalterabile** nel tempo (+ **data certa** copie e config) Presenza di log storici e di sicurezza documentabili
- Acquisizione della configurazione Active Directory
- Acquisizione log degli accessi (coerenti con segmentazione, se possibile…)
- Dimostrazione circa la creazione/originalità/valore del know how (tramite analisi comparativa, log storici, contabilizzazione temporale, etc…)

L’importanza delle policy e della documentazione

- Oltre agli aspetti tecnici di sicurezza, importanti anche quelli «**organizzativi**»
- Le **policy di utilizzo dei sistemi informativi** devono specificare livelli di sicurezza, cosa possono fare i dipendenti, cosa può fare l’azienda, etc…
  - Importante sia dimostrabile la lettura/sottoscrizione da parte dei lavoratori
- Ovvia ma a volte mancante, **informativa privacy** che specifica cosa verrà fatto dei dati dei dipendenti
- Se possibile, produrre **verbali di consegna e restituzione** asset aziendali (PC, notebook, smartphone, email, VPN, utenze, etc…)
- In caso di restituzione, spesso le grosse aziende fanno copia forense cifrata
- Produrre eventuali **schemi di rete, configurazioni di sicurezza, certificazioni, risultati di vulnerability assessment o penetration test**, etc…

Grazie per l’attenzione!