Clusit
Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY SUMMIT

Security Summit

Milano 19-20-21 marzo 2024

Behind the Scenes of a Real Attack: The Need to Elevate the Level of Security Culture

Davide Baudanza, CXO & CO-FOUNDER, @IMQ INTUITY
Martino Lessio, Principal Software Security Consultant, @IMQ Minded Security

19 Marzo 2024 orario 16:30


ASSOCIAZIONE
IMQ
IMQ
group
IMQ
CSI
IMQ intuity
IMQ MINDED SECURITY
IMQ eambiente
IMQ CERTIFICATION SHANGHAI
IMQ CERTIFICATION UK
IMQ GULF
IMQ IBERICA
IMQ POLSKA
IMQ TURKEY
IMQ CSI DEUTSCHLAND
TESTING • INSPECTION • CERTIFICATION

Davide Baudanza

CXO & CO-FOUNDER @IMQ INTUITY
UNCONVENTIONAL THINKER

Clusit
Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

ASTREA
Advanced Security, Training Research, Events Agency


IMQ
intuity
ABBIAMO UN PIANO
PER ATTACCARE LA TUA AZIENDA!
NON SEMBRA, MA E' UNA BUONA NOTIZIA!

CHI SIAMO

2016 Nasce Intuity

2020 Intuity entra nel gruppo IMQ diventando IMQ Intuity

2023 IMQ Intuity entra a far parte del consorzio ABI Lab

- +200 Clienti serviti
- Operiamo in Italia, Emirati Arabi, Spagna, Germania
- 40 Dipendenti di cui 34 tecnici
- 100% Cyber Security
- Leader nella proposizione di servizi di Red Teaming – Purple Teaming

Offensive Security Certified Professional

Offensive Security Wireless Professional

Offensive Security Experienced Penetration Tester

eLearnSecurity Web application Penetration Tester

eLearnSecurity Web application Penetration Tester eXtreme

eLearnSecurity Certified Professional Penetration Tester

Altered Security Certified Red Team Master

Zero Trust Security Red Team Operator

ISACA Risk and Information Systems Control

European Security Academy OSINT & Darkweb Investigations

ISO27001 Lead Auditor

Pentester Academy Certified Azure Red Team Professional

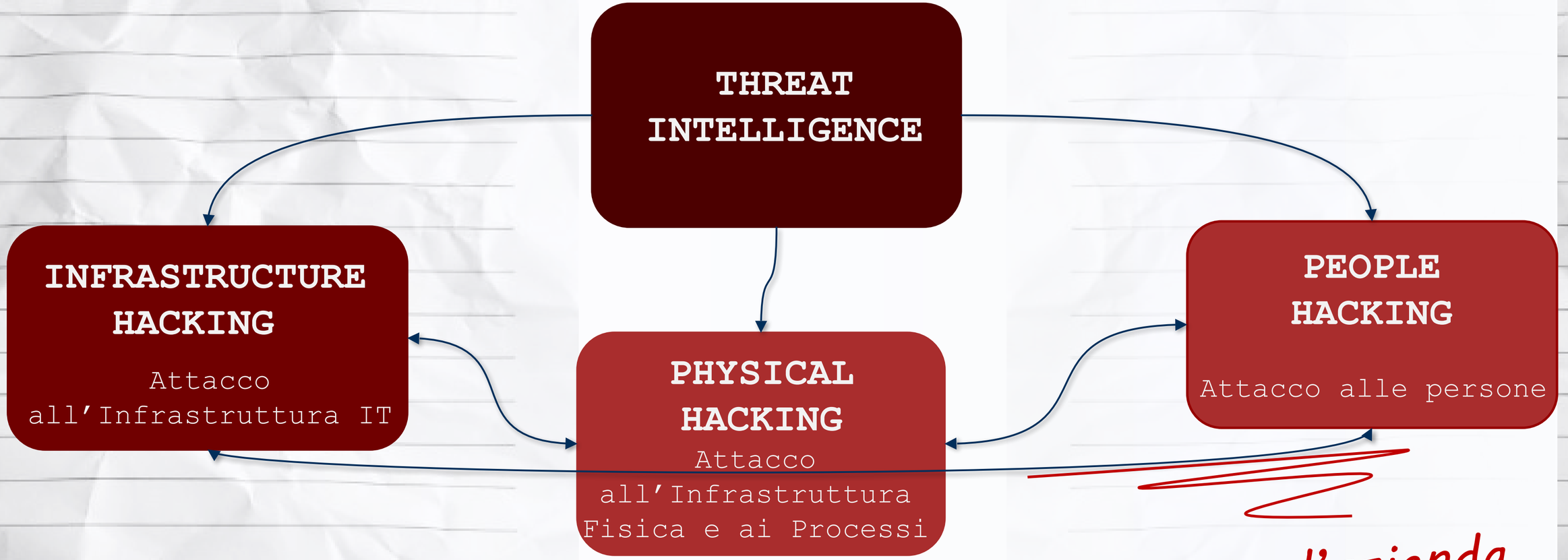
Pentester Academy Certified Red Teaming Expert

EC-Council Certified Ethical Hacker

ArcX Cyber Threat Intelligence Practitioner

ArcX Advanced Cyber Threat Intelligence

Il RED TEAM, cos'è per noi?



attaccare tutta l'azienda

IL NOSTRO APPROCCIO

- Tutte le aziende sono «digitali»
- Approccio solo tecnologico è fallimentare
- La Cyber Security è trasversale
- L'azienda fa parte di un ecosistema di aziende
- E' necessario un approccio top-down
- Il management dev'essere coinvolto attivamente
- La cyber security è un problema di **BUSINESS**
- La carenza di Cyber Security è un problema di **Cultura**

Il consueto piano d'attacco

Threat Intelligence

Identificazione elementi infrastrutturali

Profilazione organizzazione

Mappatura sedi fisiche

Ricerca informazioni rilevanti

Compromissione iniziale

Sfruttamento vulnerabilità infrastrutturali

Social Engineering, phishing\vishing

Accesso a locali e stabilimenti aziendali, *badge cloning*, *tailgating*

Azioni sull'obiettivo

Persistenza

Movimenti laterali

Privilege escalation

Raggiungimento dell'obiettivo

Installazione Ransomware-Like

Esfiltrazione dati

Fotografia di documenti e aree riservate

CASE #0001

Threat Intelligence

Identificazione **Credenziali DarkWeb** di **Consulenti Vecchio CRM**

Compromissione iniziale

Accesso CRM! Identificazione **parametri web vulnerabili a SQL Injection**!! Remote Command Ececution & Local **Privilege Escalation** su **Application Server**!!! C2C Persistence

Azioni sull'obiettivo

Password Spray su Server DMZ! **Dump Service Account** su Dominio Interno. Accesso a Server **Active Directory Privilege Escalation** tramite **ADCS** Misconfiguration **ESC1**

Raggiungimento dell'obiettivo

Accesso Dati Clienti Emissione Buoni Acquisto presso negozi
Accesso Mail Box Archive C-Level.
Exfiltration over SSL
Ransomware-Like Message su PC Utenti

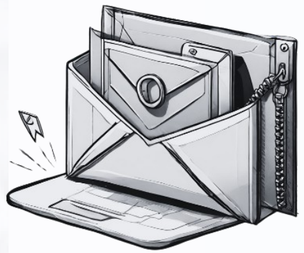
CASE #0002

Threat Intelligence

Social Sentiment su tematiche **Welfare dei Dipendenti**

Compromissione iniziale

Phishing **'Settimana Lavorativa Breve'**!
Account Breached ma con MFA **Device Code Authentication**
Posta Elettronica **utilizzata** impropriamente come un **Password Manager**



Azioni sull'obiettivo

Accesso Portale PEC
Invio Email con Allegato Zippato
Compromissione account Amministrazione
Esfiltrazione Sharepoint, Note Email, Password.

Raggiungimento dell'obiettivo

Accesso Minute del CDA!
Piano strategico APAC triennale!!
Autorizzazione Bonifico 'Simbolico' di € 5.000!!!

Giuro!!! abbiamo emesso nota di credito

CASE #0003

Threat Intelligence

Identificazione **Mobile Application Intranet** con processo di registrazione che **non prevede approvazione**

Compromissione iniziale

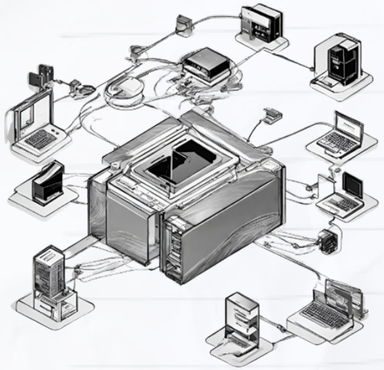
Registrazione e Accesso su MobApp Intranet.
Parametri **API** Vulnerabili a SQLi & **Broken Access Control.**
Dati personali di tutti i dipendenti registrati.
Lettura **Password.**
Accesso VPN secondaria (**no MFA**).

Azioni sull'obiettivo

Enumeration Active Directory!
Password in **Description** per **Service Account!**
Password Spray!
Local Privilege Escalation su Print Server
Dump Credenziali Domain Admin User

Raggiungimento dell'obiettivo

Accesso Amministrativo a Sistema di Backup!
Accesso a progetti brevettati.
Exfiltration over SSL
Inserimento Docker su Ambiente Tanzu/K8



Martino Lessio

Principal Software Security Consultant @ IMQ Minded Security

- ex-Dev
- MAPT, WAPT, NPT, GOPT, *PT
- SCR
- Fixing Support

Off work: guido trattori e cambio pannolini.

AGENDA

1. Mobile Security case-study

- Vulnerabilities, remediations and analysis

2. Software Security by Design

- SAMM, 5D, Threat Modeling, Secure Design, Building, Guidelines, SCR, WAPT, Fixing

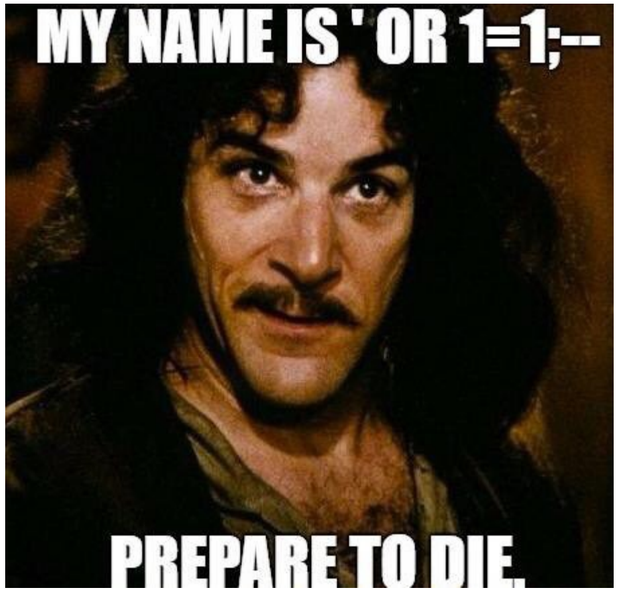
1. Case Studies

Target: Internet/Intranet Mobile application

Issue rilevate:

- Broken Access Control su layer INTRAnet
- SQL Injection
- Exfiltration Password VPN
- Password deboli
- Privilege Escalation

Risultato: Accesso Amministrativo a sistemi e dati riservati



Remediation & Next Steps

Broken Access Control: Disabilitare self registration

SQL Injection: Usare query parametriche
Accesso/Guess Pwd: Usare pwd robuste e salvate in modo sicuro

Priv Esc+Accesso Admin: Exploit non più possibile

Cosa è andato storto?

Cultura: Applicazione ingegnerizzata in modo non corretto e senza concetto di "***built-in Security***"

Review: Applicazione implementata ***senza*** una attività di CyberSecurity preliminare

Training: Gli sviluppatori non avevano ***conoscenze basilari*** di CyberSecurity

Supply Chain: ***SDLC*** era ***mancante di controlli*** sulle componenti usate

Cosa è andato storto?

Cultura: Applicazione ingegnerizzata in modo non corretto e senza concetto di Security built-in

TM

Review: Applicazione implementata senza una attività di CyberSecurity preliminare

Training: Gli sviluppatori non avevano conoscenze basilari di CyberSecurity

Supply Chain: SDLC era mancante di controlli sulle componenti importate

Cosa è andato storto?

Cultura: Applicazione ingegnerizzata in modo non corretto e senza concetto di Security built-in

TM

Review: Applicazione implementata senza una attività di CyberSecurity preliminare

Architecture Review

Training: Gli sviluppatori non avevano conoscenze basilari di CyberSecurity

Supply Chain: SDLC era mancante di controlli sulle componenti importate

Cosa è andato storto?

Cultura: Applicazione ingegnerizzata in modo non corretto e senza concetto di Security built-in

TM

Review: Applicazione implementata senza una attività di CyberSecurity preliminare

Architecture Review

Training: Gli sviluppatori non avevano conoscenze basilari di CyberSecurity

Training

Supply Chain: SDLC era mancante di controlli sulle componenti importate

Cosa è andato storto?

Cultura: Applicazione ingegnerizzata in modo non corretto e senza concetto di Security built-in

TM

Review: Applicazione implementata senza una attività di CyberSecurity preliminare

Architecture Review

Training: Gli sviluppatori non avevano conoscenze basilari di CyberSecurity

Training

Supply Chain: SDLC era mancante di controlli sulle componenti importate

SDLC Review

Mancherebbe un punto…

Controllo Continuo: Mancanza di Attività di Penetration Test

Mancherebbe un punto…

Controllo Continuo: Mancanza di Attività di Penetration Test

Secure Code Review	WAPT	MAPT
NPT	GOPT	

2. Software Security by Design

Ogni giorno in un’azienda: Dev Team

Ogni giorno in un’azienda: PM/Management

Come invece dovrebbero andare le cose:

One Ring to rule them all

One Ring to rule them all

OWASP SwSec 5D

Il Framework in pillole

- Maturity Model
- Awareness
- SAMM-Related
- Approccio Pratico
- Standard friendly (ISO 27001, NIST, SAMM, etc.)
- Self Assessment survey

Goal: SDLC Improvement

Le Dimensioni

SwSec PROCESSES

- Risk Assessment - Security Requirements
- Threat Modeling - Security Design
- SCR, WAPT, MAPT, NPT, GOPT
- Software Acceptance - Security bug Fixing

SwSec TESTING

- SAST, DAST, IAST, RASP
- External manual SCR, WAPT

SwSec TEAM

- AppSec manager/CISO, Sec Champions, AppSec Specialists, Satellite Architects, Sat Developers,Sat Testers

SwSec AWARENESS

- Management, Application Owners, Analysts, Auditors, Architects, Developers, Engineers

SwSec STANDARDS

- Sw Security Roadmap (SAMM) - Risk analysis - Threat Modeling - Sec Architecture - Sec Coding - Software Assurance

L'Output

SwSec PROCESSES

- Risk Assessment - Security Requirements
- Threat Modeling - Security Design
- SCR, WAPT, MAPT, NPT, GOPT
- Software Acceptance - Security bug Fixing

SwSec TESTING

- SAST, DAST, IAST, RASP
- External manual SCR, WAPT

SwSec TEAM

- AppSec manager/CISO, Sec Champions, AppSec Specialists, Satellite Architects, Sat Developers,Sat Testers

SwSec AWARENESS

- Management, Application Owners, Analysts, Auditors, Architects, Developers, Engineers

SwSec STANDARDS

- Sw Security Roadmap (SAMM) - Risk analysis - Threat Modeling - Sec Architecture - Sec Coding - Software Assurance

5D & SDLC

SDLC phases	Software Security Processes	Software Security Standards	Software Security Testing	Team	Awareness
Define	**Risk Assessment** **Secure Requirement**	**Sw Security Roadmap (SAMM)** **Risk analysis** **Secure Software Requirements**		**Management** **Security Champions**	**Management, IT Managers,App Owners**
Design	**Threat Modeling** **Secure Software Design**	**Threat modeling use cases** **Secure Architecture**		**Analysts** **Security Champions**	**Sec Specialists**
Develop	**Secure Code Review** **Web Application Testing** **Security Bug Fixing**	**Secure Coding Guidelines** **Outsourcing Governance (Software Assurance)**	**SAST** **DAST** **IAST** **SCR**	**DevOps** **Security Champions**	**Devs** **Sec Specialist**
Deploy	**Secure Software Testing & Acceptance** **Security Bug Fixing**	**Security Validation and Testing**	**RASP** **SCR/WAPT**	**DevOps** **Security Champions**	**Ops**
Maintain	**Secure Software Deployment & Maintenance** **Security Bug Fixing**	**Secure Deployment**	**RASP** **WAPT**	**Devops** **Security Champions**	**Sec Engineers**

5D - Goals

- Definire **dimensioni** in cui migliorare:
  - Team, Awareness, Standards, Processes, Testing
- **Misurare la cultura** della CyberSecurity con una metrica
  - Interna all'azienda
  - Dei/Verso i fornitori/clienti
- Definire una **strategia** e un **piano di azione** per la crescita
- **Certificare** i miglioramenti nel tempo

Q&A

VIENI A TROVARCI AL NOSTRO STAND!

CONTATTI:

INFO@INTUITY.IT

INFO@MINDEDSECURITY.COM