DIIES Dipartimento di
INGEGNERIA
dell'INFORMAZIONE, delle INFRASTRUTTURE e dell'ENERGIA SOSTENIBILE

Corso di Tecnologie per la sicurezza informatica

Introduzione

Principi e Norme

Vincenzo Calabrò

Principi fondamentali

“The Security Architecture is an integral and critical component within the overall architecture of an enterprise, service, product, or application.
It specifies the features and artifacts needed to protect *confidentiality*, *integrity*, and *availability* of information.”

Encyclopedia of Cryptography and Security

Approccio: "Security by Design"

Agenda

- La sicurezza informatica come asset di crescita digitale
- Enti e istituzioni a rischio: case study di rilievo
- Profiling dell'attaccante: riconoscere le diverse tipologie di “hacker”
- Figure professionali coinvolte nell'information security
- Comprendere le strategie generali di difesa e attacco
- Modelli di sicurezza: concetto di riservatezza, integrità e disponibilità
- Criteri di valutazione: vulnerabilità, rischio e impatto
- La strategia Defence In Depth: difendersi nei diversi livelli di sicurezza
- Sistemi di controllo fisico, logico e amministrativo

La sicurezza informatica come asset di crescita digitale

- Il digitale si è ormai imposto come fenomeno a larga scala e pervasivo nella comunità globale
- Non solo genera cambiamenti nelle abitudini e negli stili di vita delle persone, ma si impone anche come fattore di discontinuità nella vita delle imprese e delle organizzazioni
- Il termine “disruption”, spesso associato al digitale descrive l’impatto distruttivo sui mercati e sulle organizzazioni che devono affrontare i cambiamenti determinati dal digitale
- Tali cambiamenti, come ad esempio nel business o nella P.A., determinano il riassetto dei mercati, il change management, nuovi leader e modelli a cui adeguarsi, pena la sopravvivenza
- Pertanto, **la sicurezza dell’informazioni in formato digitale è un fattore abilitante per il successo della crescita digitale**

La sicurezza informatica come asset di crescita digitale

La sicurezza delle informazioni si può raggiungere attraverso idonei processi organizzativi.

Sono infatti necessari processi per stabilire qual è il risultato di sicurezza adeguato, individuare le carenze, decidere come colmarle e con quali prodotti, programmare i tempi e i responsabili delle attività di adeguamento, formare il personale e mantenere le soluzioni adottate.

I processi sono tra loro interrelati e interagenti per cui è necessario definire un Sistema di Gestione (management system): insieme di elementi interrelati e interagenti di un'organizzazione per stabilire politiche e obiettivi e processi per raggiungere tali obiettivi. (ISO/IEC 27000)

Cos’è la sicurezza informatica ?

- Componente
- Applicazione
- Attività
- Prodotto
- Modello
- Risorsa
- Tecnologia
- Soluzione
- Servizio

La sicurezza non è qualcosa che si può aggiungere a posteriori

Un’unica soluzione non è sufficiente

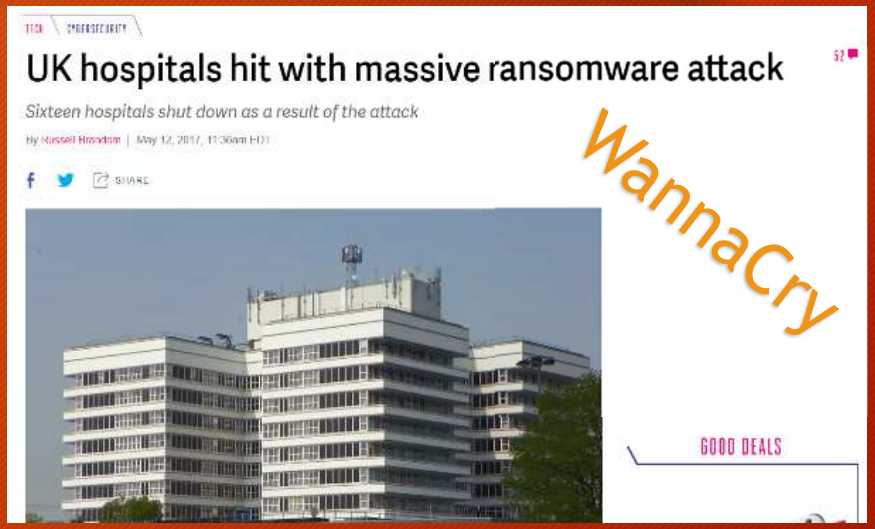
La sicurezza informatica come asset di crescita digitale

Quali sono gli elementi che impattano con la sicurezza informatica?

- **Personale / Organizzazione**
- **Processi / Procedure**
- **Prodotti / Servizi**
- **Dati / Informazioni**
- **Tecnologia**
- **Stakeholders**
- **Fornitori**
- **Clienti**
- **Contesto**
- **Livello di Rischio**
- **Concorrenti / Avversari**

Enti e istituzioni a rischio: case study di rilievo

Conficker



WannaCry

Hacked

Data Breach

Profiling dell'attaccante:
riconoscere le diverse tipologie di hacker

- **Black hat hacker**: sfruttano le vulnerabilità per finalità criminali
- **White hat hacker:** hanno fini etici, sono ingaggiati per scoprire nuove vulnerabilità e diffondo le patch di sicurezza
- **Grey hat hacker**: si limitano a trovare le vulnerabilità ed a segnalarle per fini pubblicitari
- **Hacktivist**: sono attivisti di internet, che sfruttano le loro competenze hacker a scopi politici.
- **Nation state hacker**: organizzano attacchi per favorire la propria nazione
- **Script Kiddy**: aspiranti hacker con poca esperienza che sfruttano soluzioni pronte all'uso

Security Analyst

Plan, analyse and execute cybersecurity strategies and plans

Vulnerability assessor

Spot vulnerabilities and solve them

Security Auditor

Find the weak spots in a security system before criminals do

Security Administrator

Keep security systems running smoothly

Source Code Editor

Ensure code accuracy and safety prior to release

Security Consultant

Advice and implement security solutions

Security Engineer

Build IT security systems for your organisations protection

Incident Responder

Look out for threats and actively respond to them

Forensic Expert

Protect and assist in law enforcement through a scientific study of security.

Penetration Tester

Hack into computer and network systems to preemptively discover operating system vulnerabilities, service and application problems, improper configurations and more

IT Security Consultant

Meet with clients to advise them on how to best protect their organizations' cyber security objectives efficiently and cost effectively.

Chief Information Security Officer

The chief information security officer (CISO) is typically a mid-executive level position who oversees the general operations of a company's or organization's IT security division. CISOs are directly responsible for planning, coordinating and directing all computer, network and data security needs of their employers.

Figure professionali coinvolte nell'information security

Comprendere le strategie generali di difesa e attacco

La Sicurezza informatica come leva strategica di innovazione e crescita deve prevedere una metodologia codificata.

I primi passi contemplano le attività per innalzare i livelli di sicurezza:

- Analisi e valutazione delle minacce e delle vulnerabilità
- Implementazione delle misure di sicurezza per mitigare i rischi
- Attivazione di sistemi per il monitoraggio e il rilevamento degli incidenti
- Avviamento delle misure per il contenimento e il ripristino

Le attuali tendenze affiancano anche strategie di attacco:

- Ricerca di nuove vulnerabilità
- Test della risposta agli attacchi
- Verifica della resilienza dell'organizzazione

Comprendere le strategie generali di difesa e attacco

Modelli di sicurezza: concetto di riservatezza, integrità e disponibilità

Il modello classico della sicurezza delle informazioni definisce tre obiettivi di sicurezza:

- **Riservatezza (confidentiality)** significa proteggere le informazioni dagli accessi da parte di soggetti non autorizzati.
- **Integrità (integrity)** vuol dire garantire l'autenticità dell'informazione, che tale informazione non sia alterata e che la sorgente dell'informazione sia autentica.
- **Disponibilità (availability)** significa che l'informazione è accessibile agli utenti autorizzati.

Oltre alle tre fondamentali proprietà possono essere considerate anche: **Autenticità, Completezza, Non ripudiabilità, Responsabilità, Affidabilità, Resilienza, Continuità Operativa.**

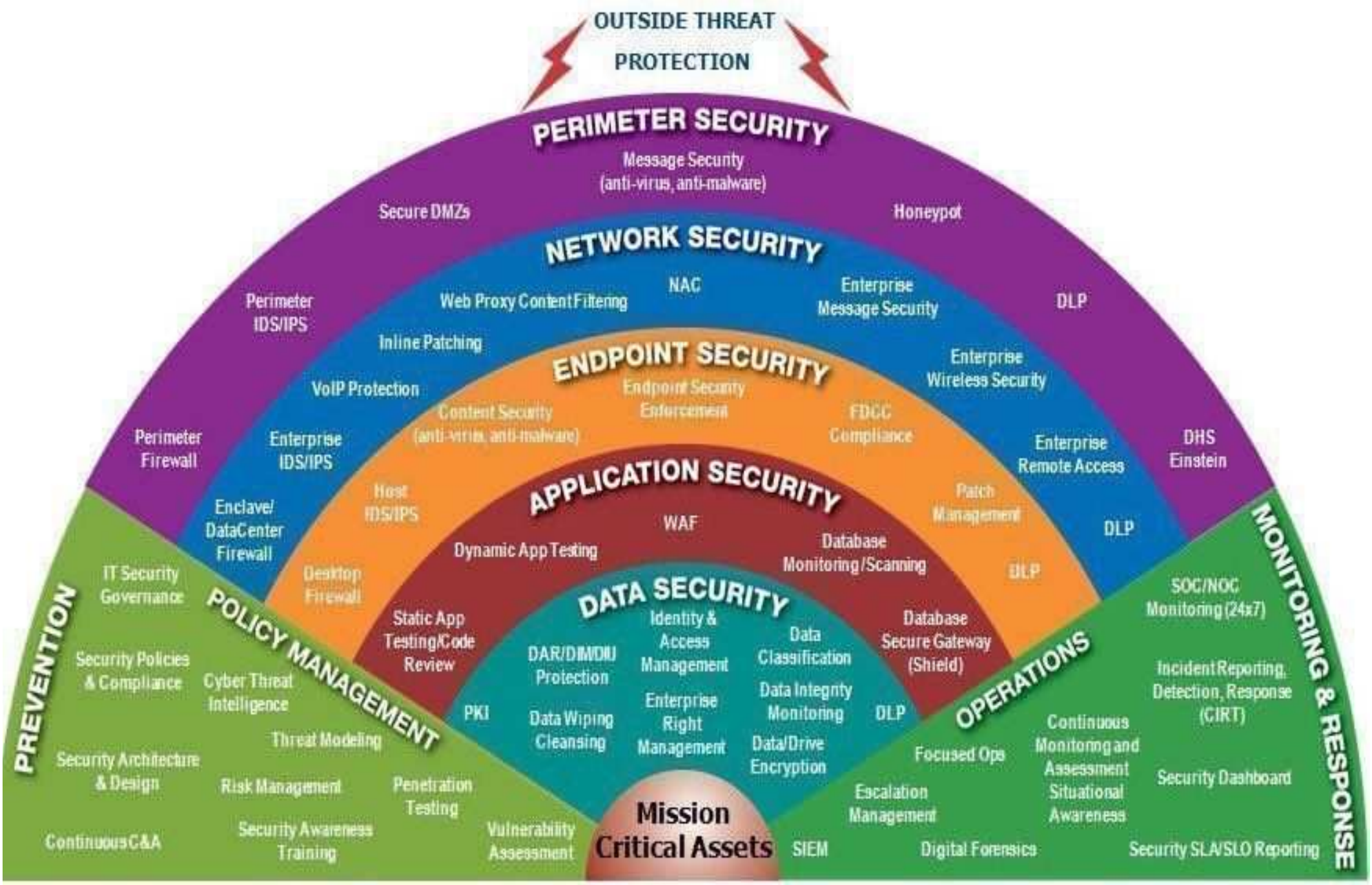
Criteri di valutazione dei rischi: vulnerabilità, rischio e impatto

Una metodologia di valutazione dei rischi per la sicurezza delle informazioni comprende le seguenti fasi:

1. Identificazione dei rischi (vulnerability analysis / penetration test)
2. Analisi e ponderazione dei rischi
3. Identificazione e valutazione delle opzioni per il trattamento dei rischi
4. Scelta degli obiettivi di controllo ed i controlli per il trattamento dei rischi
5. Accettazione dei rischi residui

Le attività suddette vengono descritte nel Rapporto di valutazione dei rischi (Risk assessment report).

Impatto = Valore Asset x Gravità Minaccia x Gravità Vulnerabilità



La strategia Defence In Depth: difendersi nei diversi livelli di sicurezza

Sistemi di controllo fisico, logico e amministrativo

Sistemi di controllo fisico:

- Sistemi di sicurezza perimetrali
- Sicurezza delle comunicazioni (firewall, ids, ecc.)

Sistemi di controllo logico

- Controlli degli accessi e delle autorizzazioni
- Crittografia
- Backup
- Raccolta log e monitoraggio

Sistemi di controllo amministrativo

- Procedure operative e responsabilità
- Gestione degli incidenti
- Continuità operativa della sicurezza

Vulnerabilità e falle di sicurezza tipiche

- Software e dispositivi non aggiornati, obsoleti o non mantenuti
- Configurazioni di default, improprie o deboli
- Gestione impropria dell'autenticazione e dell'input utente
- Connessioni e sistemi di crittografia insicuri
- Errata gestione dei certificati e delle chiavi
- Architettura informatica debole e insicura
- Utenti inesperti e procedure vulnerabili o assenti
- Presenza di software e dispositivi non autorizzati
- Minacce interne e mancati controlli sul personale
- Nuovi attacchi e Zero Day

Attacchi informatici e Malware

- **Attaccare le reti informatiche**: Man-in-The-Middle, Spoofing, DDos, Amplification, Replay
- **Attaccare le applicazioni e il sistema operativo**: Buffer Overlow, Zero Day, Privilege Escalation
- **Attaccare i siti e le applicazioni web**: SQL Injection, Cross-site Scripting, Session Hijacking
- **Attaccare le password e i sistemi crittografici**: Bruteforce, Dictonary, Rainbow Tables, Collision, Downgrade
- **Attaccare gli utenti attraverso ingegneria sociale**: Phisting, Vishing, Tailgating, Impersonation
- **Attacchi attraverso malware**: Virus, Worm, Trojan, Ransomware, etc

Fasi e dinamiche di un attacco informatico mirato

La **Cyber Kill Chain** descrive un modello a fasi utile a identificare un cyber attacco dal punto di vista dell'attaccante (pensare come un hacker). Sviluppato da Lockheed Martin per scenari militari, il modello è composto da una serie di fasi predefinite che individuano la posizione dell'attaccante nei confronti della vittima:

1. **Reconnaissance**: ricerca le vulnerabilità e sviluppa un piano di attacco
2. **Armament**: è creato/individuato l'exploit da utilizzare per l'attacco
3. **Delivery**: l'exploit viene recapitato tramite un vettore di attacco
4. **Exploitation**: il malware sfrutta una falla per portare a segno l'attacco
5. **Installation**: il payload viene scaricato e installato
6. **Command and Control**: l'entità che viene contattata dal malware per inviare dati raccolti dalla vittima o ricevere nuove istruzioni
7. **System Compromise**: il sistema può essere utilizzato per altri attacchi

Tecniche di difesa e contromisure

- **Proteggere la rete e le connessioni riservate**: VLAN, DMZ, VPN, SSL, Firewall, Antivirus
- **Proteggere i software e il sistema operativo**: Hardening, Logs e aggiornamenti, Sandboxing
- **Proteggere i dati sensibili e la postazione di lavoro**: Crittografia, Shredding, Hardening Firmware, TPM
- **Garantire la continuità del servizio**: Backup, Disaster Recovery, Mirroring e ridondanza
- **Garantire la corretta autenticazione e il controllo d'accesso**: Autenticazione multi-fattore, biometrica, password e chiavi
- **Sistemi e dispositivi per la sicurezza fisica**
- **Tecniche e strategie di prevenzione**: IDS/IPS, Log analysis e monitoring, scansione vulnerabilità
- **Analisi e Gestione del rischio e degli incidenti**
- **Formulare procedure formali e sensibilizzare gli utenti**

Strumenti di attacco alla Sicurezza Informatica

- Strumenti fondamentali a linea di comando e linguaggi di scripting
- Sistemi operativi e distribuzioni dedicate alla sicurezza informatica
- Fonti di consultazione e strumenti utili nel web
- Analizzatori di traffico e mappatura della rete
- Scansionatori di vulnerabilità e Framework per l'exploitazione
- Database di malware, exploit e vulnerabilità note
- Utilizzo di proxy e connessioni anonime
- Honeypot e ambienti di simulazione

Dalla sicurezza informatica alla cyber security

- **Sicurezza informatica**: incentrata sui dati, in termini di disponibilità, confidenzialità e integrità

- **Cyber security**: oltre ai dati, include lo spazio cibernetico, inteso come luogo virtuale nel quale opera la sicurezza informatica, gli attacchi informatici ai dati, reti, software, infrastrutture, organizzazioni, ecc.

La cybersecurity e la disciplina in ambito internazionale

Le costanti minacce a cui sono sottoposti i sistemi informatici hanno contribuito alla crescita d'interesse verso i temi della «***cybersecurity***» e «***ciberdefence***»

Si distinguono diversi tipi di norme:

- **Linee guida**: manuali o raccolte di best practices disponibili per una loro selezione al fine di raggiungere un certo obiettivo
- **Standard verificabili**: norme con specifiche rispetto alle quali può essere condotto un audit da parte di personale indipendente

Linee guida internazionali:

- OCSE sulla sicurezza dei sistemi e delle reti di informazione (1992)

Standard internazionali:

- **ISO** - International Organization for Standardization: ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection
- **NIST** - National institute of Standard and Technology: Cyber Security Framework
- **ISA** - International Society of Automation: ISA/IEC 62443 Cybersecurity Certificate Programs

Le norme della famiglia ISO/IEC 27000

La ISO/IEC 27001 è uno ***standard verificabile***. Possono essere condotti audit di un sistema di gestione per la sicurezza delle informazioni di un'organizzazione e, se questo è ritenuto conforme ai requisiti della ISO/IEC 27001, può essere emesso un certificato di conformità.

La ISO/IEC 27001 è affiancata da altre ***linee guida*** che forniscono supporto all'attuazione dei suoi requisiti o delle indicazioni per la sua applicazione in settori specifici. L'insieme di queste norme è detto famiglia delle norme ISO/IEC 27000 (ISMS standard family o famiglia di norme dei SGSI) e ne fanno parte:

- ISO/IEC 27002: guida per la scelta dei controlli di sicurezza
- ISO/IEC 27003: guida all'interpretazione dei requisiti della ISO/IEC 27001
- ISO/IEC 27004: guida per la misurazione e il monitoraggio di un sistema di gestione per la sicurezza delle informazioni
- ISO/IEC 27005: guida per la valutazione e gestione del rischio relativo alla sicurezza delle informazioni

Le norme della famiglia ISO/IEC 27000

Altre norme della famiglia sono quelle che estendono i controlli della ISO/IEC 27001 e ne fanno parte:

- ISO/IEC 27011: con controlli di sicurezza attuabili dai fornitori di servizi di telecomunicazioni
- ISO/IEC 27017: con controlli di sicurezza attuabili dai fornitori e dagli utilizzatori del cloud
- ISO/IEC 27018: con controlli privacy attuabili dai fornitori di servizi cloud
- ISO/IEC 27019: con controlli di sicurezza attuabili nel settore dell'energia
- ISO 27799: con controlli di sicurezza attuabili nel settore della sanità
- ISO/IEC 29151: per i titolari dei trattamenti dei dati personali
- ISO/IEC 27701: la certificazione del sistema di gestione per la protezione dei dati personali, ispirato al Regolamento europeo sulla protezione dei dati personali

La disciplina europea della cybersecurity

La cybersecurity è divenuta per l'Unione Europe una garanzia a tutela del Mercato Unico Digitale (Digital Single Market).

Provvedimenti principali:

- Istituzione dell'Agenzia Europea di sicurezza delle reti e dell'informazione (ENISA) (2004)
- Libro verde: sicurezza delle infrastrutture critiche (2005)
- Direttiva Infrastrutture Critiche europee e per la loro protezione (2008)
- Direttiva misure di sicurezza nel campo delle comunicazioni elettroniche (2009)
- Strategia dell'Unione Europe per la sicurezza cibernetica (2013)
- Direttiva sicurezza delle reti e dell'informazione – NIS (2016)
- Regolamento General Data Protection Regulation – GDPR (2016)
- Cybersecurity Act (2019)

Normative per la Sicurezza Informatica e Data Protection

Stato attuale della legislazione comunitaria:

- il Regolamento n. 679/2016, **Regolamento Generale sulla Protezione dei Dati (RGPD)**, entrato in vigore il 24 maggio 2016, applicabile dal 24 maggio 2018, che sostituisce la Direttiva 95/46/CE
- il Regolamento n. 910/2014, **Regolamento Electronic Identification Authentication and Signature (Regolamento EIDAS)**, entrato in vigore il 17 settembre 2014, applicabile dal primo luglio 2016, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, che sostituisce il quadro normativo definito dalla Direttiva Europea 1999/93/EC
- la Direttiva n. 680/2016, **Direttiva sul trattamento dei dati personali da parte delle autorità competenti** a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, entrata in vigore il 24 maggio 2016, che abroga la decisione quadro 2008/977/GAI del Consiglio
- la Direttiva n. 1148/2016, **Direttiva Network and Information Security (Direttiva NIS)**, entrata in vigore l'8 agosto 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione
- il Regolamento n. 881/2019, il **Cybersecurity Act**, entrata in vigore il 27 giugno 2019, crea un nuovo sistema di certificazione della sicurezza di prodotti e servizi ICT e che rafforza il ruolo dell'ENISA

La disciplina italiana in tema di cybersecurity

L'ordinamento italiano ha una corposa normativa per affrontare le problematiche connesse alla sicurezza informatica.

Norme principale:

- Direttiva 16/1/2002: «**Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni**»
- D.lgs 196/2003 e GDPR: «**Normativa sulla privacy e tutela dei dati personali**»
- D.LGS. 7.3.2005, art. 71 CAD «**Regole tecniche da adottare per garantire una efficace protezione dei dati e dei livelli di sicurezza necessari.**» (agg. 2017)
- DPCM 24.1.2013 «**Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali**» (agg. nel 2017)
- DPCM 17.2.2017 «**Piano nazionale per la protezione cibernetica e la sicurezza informatica**» (2017)
- Circolare AgID n. 2/2017: «**Misure minime di sicurezza ICT per le pubbliche amministrazioni**»
- D.LGS. 65/2018 «**Misure per un livello comune elevato di sicurezza delle reti e dei sistemi informatici dell'Unione (NIS)**» (2018)
- L. 133/2019 «**Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica**» (2019)

Moduli del Programma

Offensive Security

- Penetration Test dei Sistemi e dei Servizi
- Penetration Test delle Web App

Defensive Security

- Security Monitoring
- Incident Response
- Digital Forensics

“I am convinced that there are only two types of companies: those that have been hacked and those that will be. And they are converged into one category: companies that have been hacked and will be hacked again.”

Robert Mueller, Direttore del FBI, 2012

Molto probabilmente oggi quelle aziende saranno state tutte attaccate. Per cui il vero problema non è se verremo attaccati, ma quando e quante volte.

“Security is a process, not a product” Bruce Schneier, 2000

Fine

vincenzo.calabro@unirc.it
linkedin.com/in/vincenzocalabro

“Security is more than a process. It’s a proficiency.” Lance Hayden, 2016