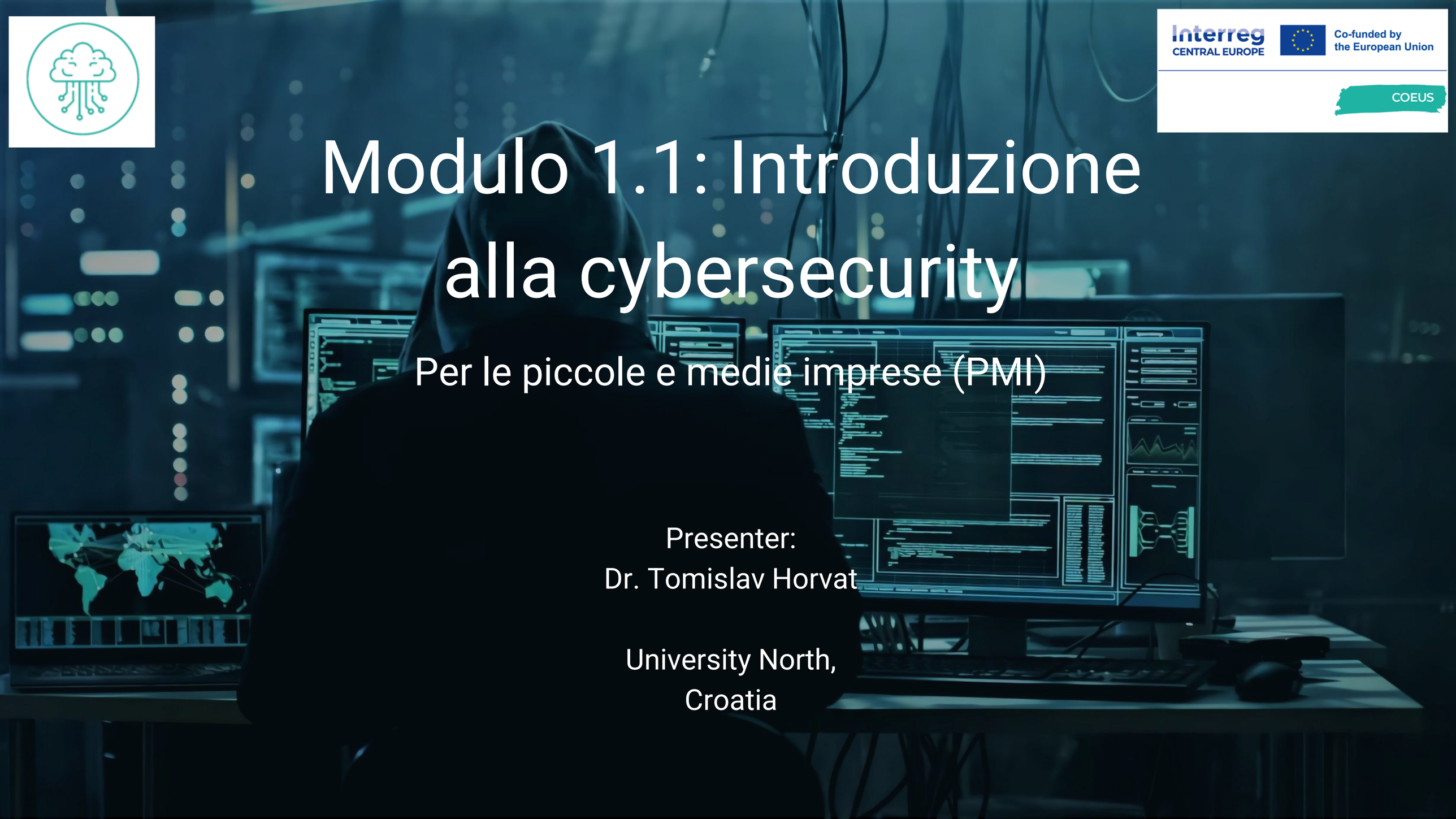
Modulo 1.1: Introduzione alla Cybersecurity

Interreg CENTRAL EUROPE
Co-funded by the European Union
COEUS



Modulo 1.1: Introduzione alla cybersecurity

Per le piccole e medie imprese (PMI)

Presenter:
Dr. Tomislav Horvat

University North,
Croatia

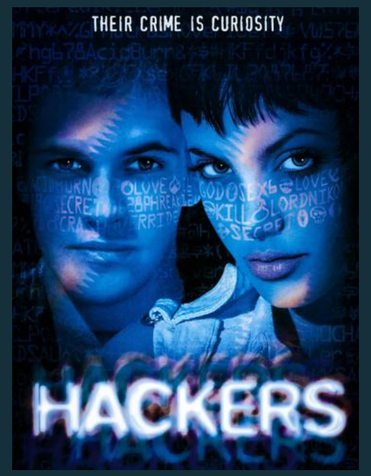
Interreg CENTRAL EUROPE
Co-funded by the European Union
COEUS

Hackers

Hackers

Il termine "hack" è nato al MIT, che significa modifiche tecniche giocose e intelligenti da parte dei primi appassionati di tecnologia.

1950



1995

1999

Il termine "hacker" oggi si riferisce a individui che vanno dai criminali informatici malintenzionati (black hat) agli hacker etici (white hat).

2024

Tipi di hacker oggi

Tipi di hacker oggi

01 Script Kiddies, o hobbisti: hacker inesperti che utilizzano strumenti predefiniti per sfruttare le vulnerabilità senza comprendere appieno la tecnologia

02 Hacktivisti - politicamente o socialmente, prendono di mira organizzazioni e governi per promuovere le loro convinzioni (defacement di siti web, attacchi DDoS, ...)

03 White Hat Hacker - lavorano legalmente per identificare e correggere le falle di sicurezza, spesso assunte dalle organizzazioni per migliorare la propria sicurezza informatica

04 Hacker Grey Hat - operano tra l'etico e il non etico, irrompono senza permesso ma di solito segnalano i problemi che trovano

05 Black Hat Hackers - hacker malintenzionati irrompono nei sistemi per guadagno personale, rubando dati e causando danni

06 Hacker sponsorizzati dallo stato: conducono spionaggio informatico, sorveglianza e guerra informatica per conto dei governi

Storia della Cybersecurity

Storia della Cybersecurity

The Morris Worm (1988)

Un momento cruciale nella sicurezza informatica, che ha messo in luce le vulnerabilità del sistema, ha portato alla creazione del primo CERT e ha portato a un'azione legale ai sensi del Computer Fraud and Abuse Act.

2010s

I dispositivi mobili e l'IoT hanno ampliato le superfici di attacco, le violazioni di alto profilo hanno sottolineato l'impatto della sicurezza informatica sulla privacy e l'intelligenza artificiale ha iniziato a migliorare il rilevamento delle minacce.

"ILOVEYOU" virus

La crescita di Internet ha portato allo sviluppo di antivirus e firewall, mentre i principali attacchi dei primi anni 2000 hanno sottolineato la necessità di misure di sicurezza più forti e di una maggiore consapevolezza pubblica.

The 2011 Stuxnet attack

L'attacco Stuxnet alla struttura iraniana di Natanz è stato fondamentale, dimostrando il potenziale degli attacchi informatici per danni fisici e rimodellando le strategie di difesa nazionale.

Trasformazione digitale

Ha ampliato la superficie di attacco, spingendo le aziende a investire in protocolli di sicurezza avanzati, formazione dei dipendenti e piani di risposta agli incidenti.

Metà -2000

La sicurezza informatica è diventata una priorità, con l'introduzione del PCI DSS nel 2004 per la protezione dei dati e l'ascesa dei social media che richiedono strategie di sicurezza avanzate.

L'ascesa del cloud computing

Ha trasformato l'archiviazione e l'elaborazione dei dati, offrendo flessibilità ma introducendo sfide in termini di privacy e conformità dei dati, portando le aziende ad adottare protocolli di sicurezza specializzati.

Che cos'è la cybersecurity?

Che cos'è la Cybersecurity?

Cybersecurity

Cyber + sicurezza = combinati si riferiscono alla protezione del nostro mondo digitale, compresi i computer,
reti, software e attività relative a Internet.

Definizione di Cybersecurity

Definizione di Cybersecurity

La sicurezza informatica si riferisce alla protezione del nostro mondo digitale, inclusi computer, reti, software e attività legate a Internet.

I dati sensibili vengono regolarmente rubati

Le aziende sono paralizzate dal ransomware

Le infrastrutture critiche vengono sabotate da malintenzionati

Capire la Cybersecurity

La cybersecurity copre un'ampia gamma di pratiche.

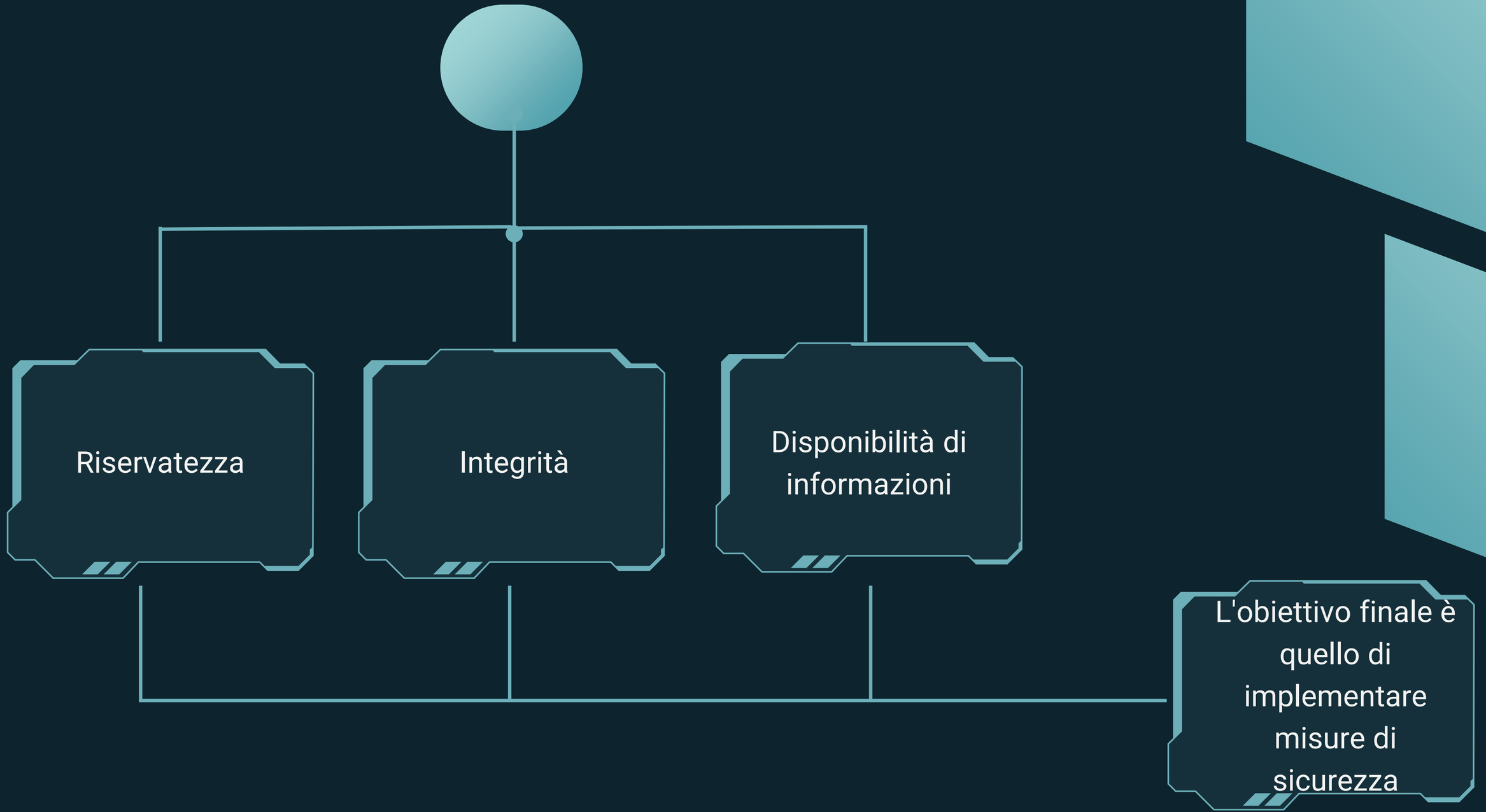
Protezione dell'integrità dei dati

Garantire la privacy

Protezione di reti e sistemi da accessi non autorizzati

L'obiettivo della Cybersecurity

L'obiettivo della Cybersecurity



L’importanza della Cybersecurity

Protezione finanziaria

- Gli attacchi informatici costano tra gli 84.000 e i 148.000 dollari
- interruzioni dell'attività, costi di recupero e perdita di produttività, ...

Protezione della reputazione

- la fiducia è vitale per le PMI
- Una reputazione danneggiata può avere effetti duraturi
- la comunicazione aiuta le PMI a mantenere la fiducia dei clienti

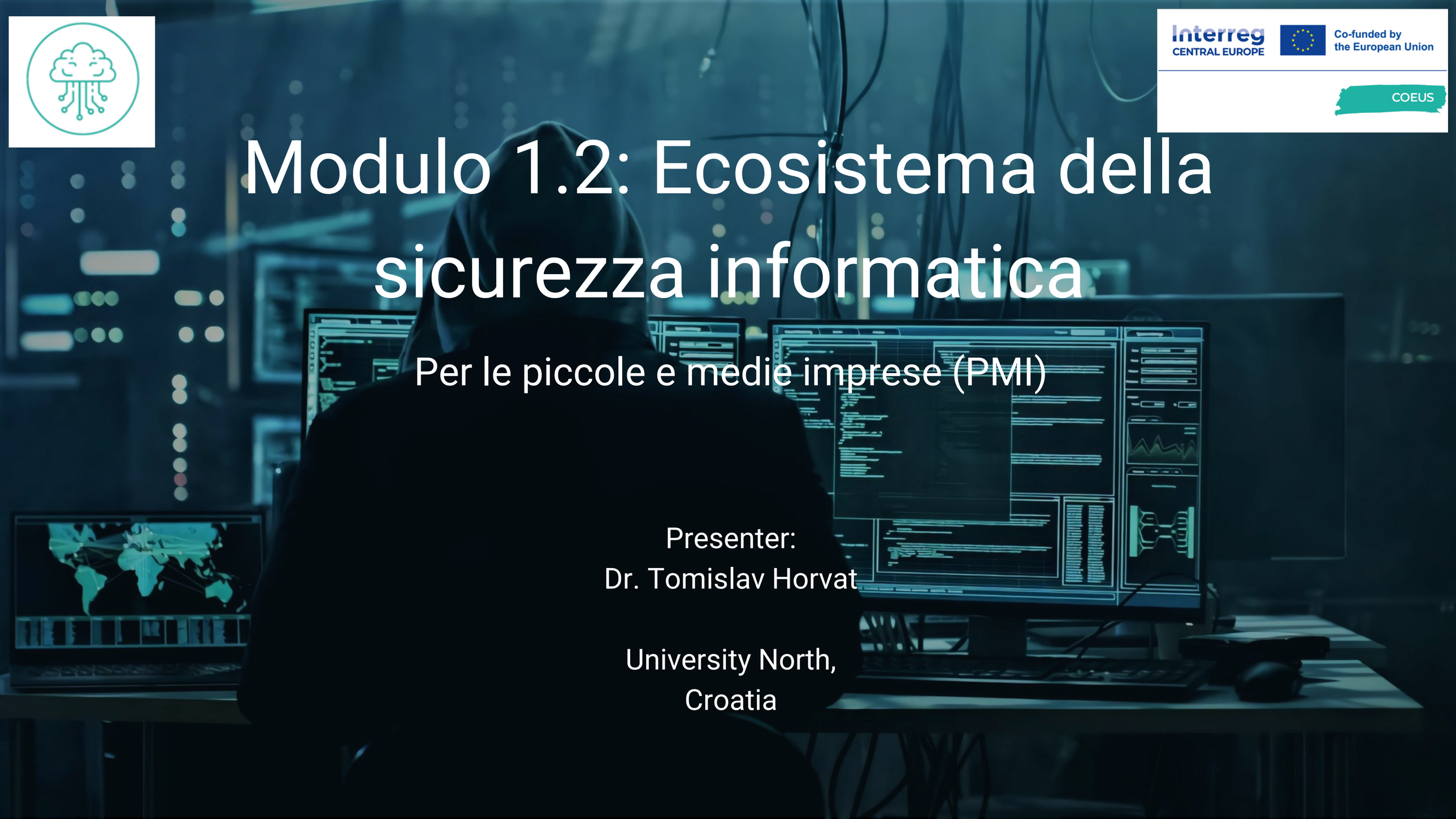
Conformità legale

- La conformità è una necessità legale
- Il GDPR protegge la privacy dei dati e la mancata conformità può portare a multe e azioni legali

Business Continuity

- Mantenere le operazioni in esecuzione è fondamentale
- La pianificazione del ripristino riduce al minimo l'impatto e accelera il ritorno all'attività

- La sicurezza informatica non è solo una questione tecnica per le PMI, ma riguarda la protezione delle loro finanze, della loro reputazione, della loro posizione legale e della loro capacità di tenere le porte aperte



Modulo 1.2: Ecosistema della sicurezza informatica

Per le piccole e medie imprese (PMI)

Presenter:
Dr. Tomislav Horvat

University North,
Croatia

Interreg CENTRAL EUROPE
Co-funded by the European Union
COEUS

Ecosistema della cybersecurity

Ecosistema della cybersecurity

Un ecosistema di sicurezza informatica è definito come una rete complessa di software, hardware, risorse di rete e utenti interconnessi che funzionano insieme come un'unità coesa.

=

Componenti tecnologici

Applicazioni, sistemi operativi, dispositivi, servizi cloud e interazioni tra di essi.

+

Persone coinvolte

Sviluppatori, utenti finali, fornitori di servizi e altre parti interessate come gli hacker etici che contribuiscono e utilizzano queste tecnologie.

Ecosistema della cybersecurity

L'ecosistema della cybersecurity è una rete complessa e interconnessa di tecnologie, processi e stakeholder finalizzata alla protezione degli asset digitali dalle minacce informatiche.

Cinque aree chiave:

01 Attori delle minacce

02 Minacce informatiche

03 Misure di sicurezza

04 Regolamenti e standard

05 Risposta

Attori delle minacce

Minacce informatiche

Malware

Un software progettato per danneggiare, sfruttare o ottenere l'accesso non autorizzato ai sistemi informatici.

Phishing

Una truffa in cui gli aggressori si spacciano per entità affidabili per ingannare le persone.

Ransomware

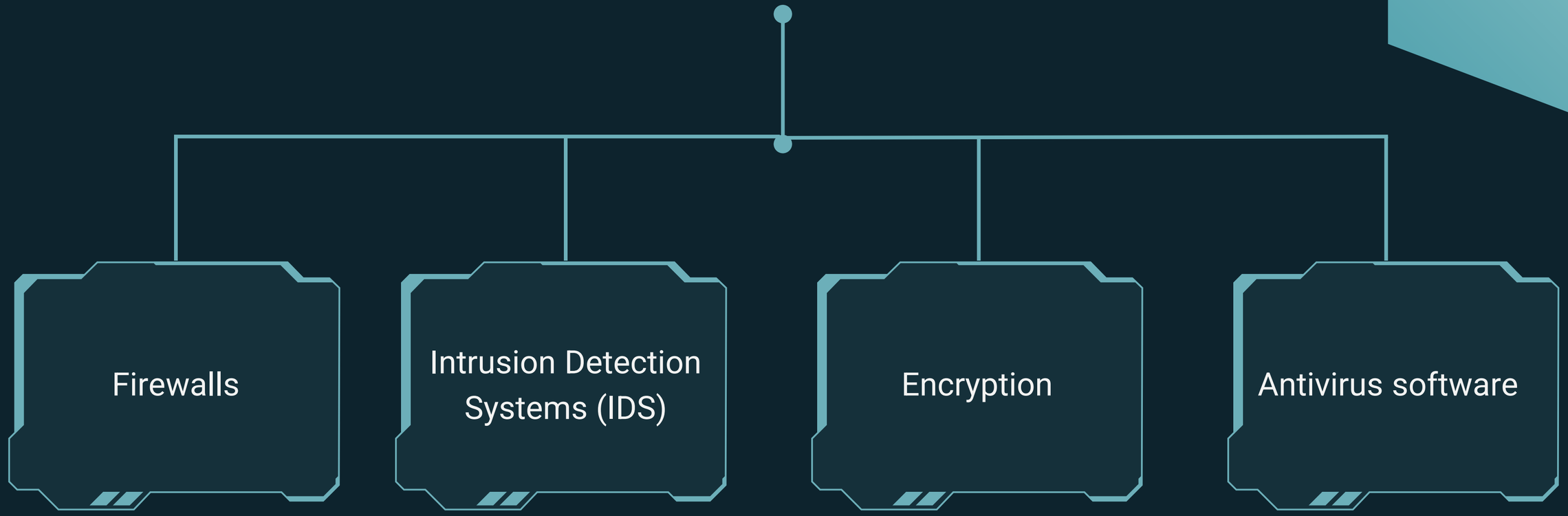
Tipo di malware che crittografa i dati di una vittima e richiede il pagamento per la chiave di decrittazione.

Attacchi DDoS

Attacchi che inondano una rete o un server con traffico eccessivo, rendendolo lento o non disponibile.

Misure di sicurezza

Misure di sicurezza



Regolamenti e standard

Regolamenti e standard

GDPR and HIPAA

Applica rigorosi protocolli di protezione dei dati e privacy.

PCI-DSS e ISO/IEC 27001

Framework per la gestione sicura delle informazioni sensibili, garantendo che le aziende mantengano solide pratiche di sicurezza delle informazioni.

Incident Response

Incident Response

Detection
Primo passo durante il quale è fondamentale identificare le anomalie che indicano una potenziale violazione.

Contenimento ed eradicazione
Isolare la minaccia e rimuoverne la causa.

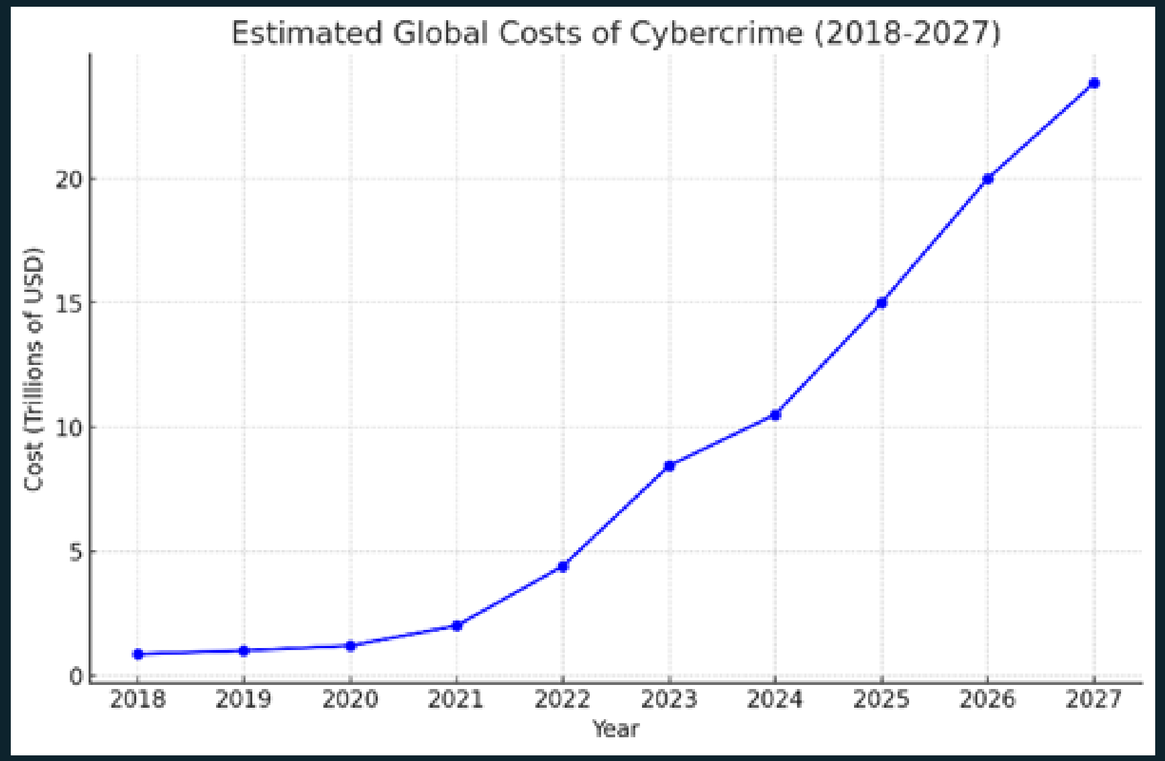
Ripristino
Ripristina i sistemi al normale funzionamento, assicurandone la sicurezza e il funzionamento.

Analisi post-incidente
Apprendimento (identificazione delle lacune, miglioramento delle strategie di risposta future).

Stima dei costi globali del crimine informatico

Stima dei costi globali del crimine informatico

- Statista stima che i costi globali del crimine informatico siano aumentati vertiginosamente da 860 miliardi di dollari nel 2018 a 23,84 trilioni di dollari previsti entro il 2027



Fonte: Statista

Assicurazione Cyber

Che cos'è l'assicurazione cyber?

L'assicurazione cyber è una copertura che protegge dai costi degli attacchi informatici, tra cui il recupero, le spese legali e i danni alla reputazione.

Copertura di responsabilità civile

Copre le spese legali derivanti da cause legali, accordi e multe dopo una violazione dei dati.

Copertura di prima parte

Gestisce perdite come il recupero dei dati, le riparazioni del sistema, l'interruzione dell'attività e persino il pagamento di riscatti.

Supporto per la risposta agli incidenti

Offre l'accesso a esperti, consulenti legali e professionisti delle pubbliche relazioni.

Gestione del rischio

Fornisci valutazioni dei rischi e risorse, come la formazione dei dipendenti e gli audit di sicurezza.

Modulo 2: Minacce informatiche e attacchi informatici

Per le piccole e medie imprese (PMI)

Presenter:
Dr. Tomislav Horvat

University North,
Croatia

Interreg CENTRAL EUROPE
Co-funded by the European Union
COEUS

Miancce Cyber vs Attacchi Cyber

Minacce Cyber vs attacchi Cyber

Minacce Cyber

- rappresentano rischi potenziali
- Malware, phishing, vulnerabilità del software o tattiche di ingegneria sociale
- Passivo di natura

VS

Cyber Attacks

- azioni deliberate intraprese da individui o organizzazioni per sfruttare queste minacce
- attivo e intenzionale
- attacchi ransomware, attacchi DDos

Tipi di minacce cyber

Tipi di minacce cyber

01 Malware

02 Phising

03 Ingegneria sociale

04 Attacchi DDoS (Distributed Denial of Service)

05 Minacce interne

Che cos'è il malware?

Che cos'è il malware?

Il malware, abbreviazione di "software dannoso", è progettato per danneggiare, rubare dati o interrompere le normali operazioni del computer.

Virus

- collegarsi a programmi legittimi e diffondersi ogni volta che tali programmi vengono eseguiti

Worms

- Autoreplicante e diffuso su reti in modo indipendente, senza bisogno dell'intervento dell'utente

Ransomware

- crittografa i dati sui sistemi infetti e richiede il pagamento di un riscatto

Spyware

- traccia e registra le attività degli utenti a loro insaputa, spesso utilizzate per rubare informazioni

Esempi di attacchi malware

Esempi di attacchi malware

01

WanaCry (2017)
massiccio attacco ransomware che ha colpito migliaia di computer in tutto il mondo

- Una volta infettata una macchina, crittografava i file e visualizzava un messaggio che richiedeva un pagamento in criptovaluta per sbloccarli
- ha reso i computer inutilizzabili, bloccando essenzialmente gli utenti fino a quando il riscatto non è stato pagato o il sistema è stato ripristinato da un backup

02

ILOVEYOU (2000)
diffuso inviando una mail con oggetto "ILOVEYOU" e un allegato

- una volta aperto, l'allegato eseguiva uno script che sovrascriveva i file e poi si inviava a tutti i contatti della rubrica di Microsoft Outlook
- I computer infetti hanno subito la perdita di dati a causa della sovrascrittura dei file, dell'instabilità del sistema e di gravi rallentamenti della rete a causa della distribuzione di massa delle e-mail

Che cos'è il phishing?

Che cos'è il phishing?

Il phishing è un tipo di minaccia informatica che utilizza comunicazioni ingannevoli, in genere tramite e-mail, per indurre le persone a rivelare informazioni sensibili, come password, dettagli della carta di credito e altri dati personali.

Email Phishing

- e-mail false generiche che sembrano provenire da organizzazioni rispettabili

Spear Phishing

- tentativi di phishing altamente mirati rivolti a individui o organizzazioni specifici, spesso utilizzando informazioni personalizzate

Whaling

- attacchi di phishing diretti a individui di alto rango all'interno delle organizzazioni, a causa del potenziale di informazioni di alto valore

Esempio di attacco di phishing

Esempio di attacco di phishing

01

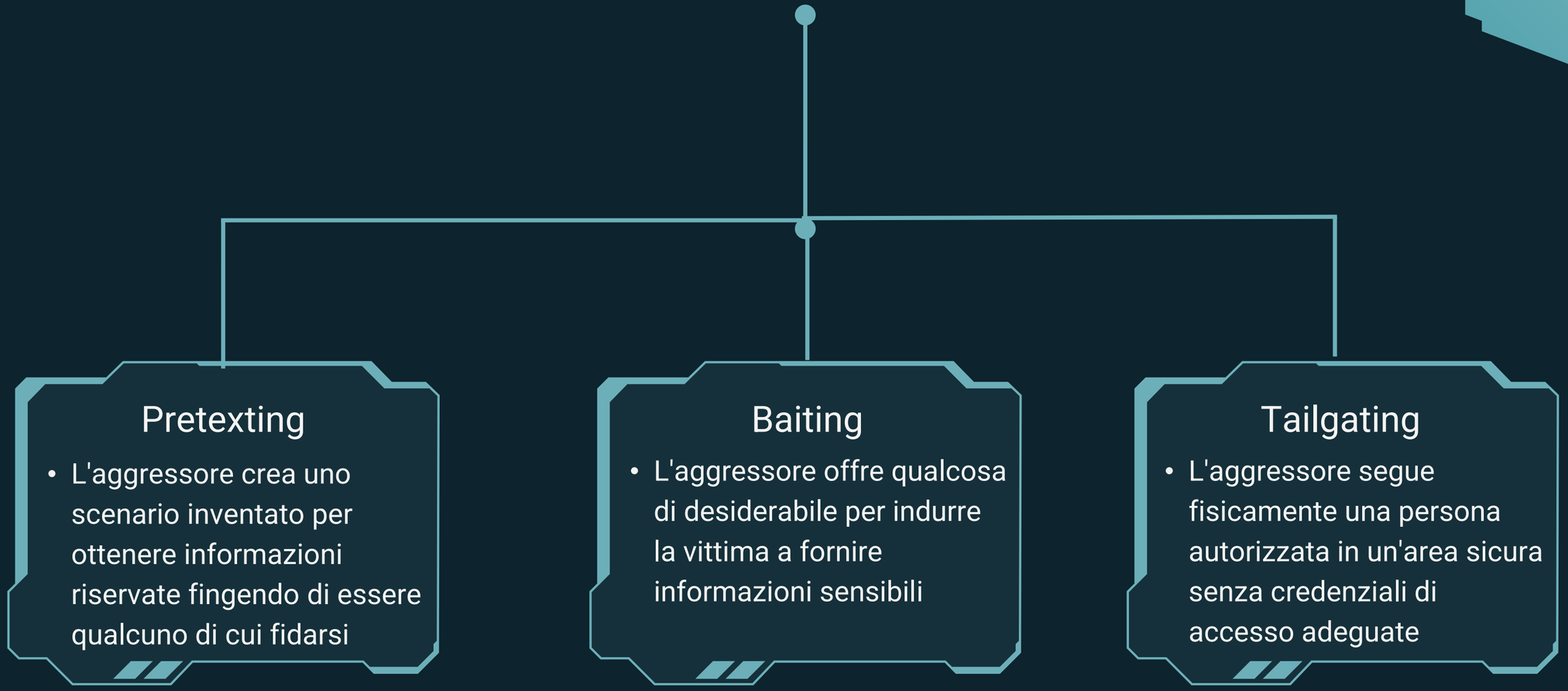
Truffa di phishing PayPal
gli aggressori hanno inviato e-mail che sembravano provenire da PayPal, esortando i destinatari a verificare i propri account o avvertendo che i loro account erano stati compromessi

- gli utenti sono stati reindirizzati a un sito Web falso che imitava la pagina di accesso di PayPal
- Le vittime hanno inconsapevolmente concesso agli aggressori l'accesso ai loro account, portando a transazioni non autorizzate e potenzialmente anche al furto di identità

Che cos'è l'ingegneria sociale?

Che cos'è l'ingegneria sociale?

L'ingegneria sociale è un tipo di minaccia informatica che manipola gli individui per rivelare informazioni sensibili o eseguire azioni che compromettono la sicurezza.



Pretexting

- L'aggressore crea uno scenario inventato per ottenere informazioni riservate fingendo di essere qualcuno di cui fidarsi

Baiting

- L'aggressore offre qualcosa di desiderabile per indurre la vittima a fornire informazioni sensibili

Tailgating

- L'aggressore segue fisicamente una persona autorizzata in un'area sicura senza credenziali di accesso adeguate

Esempio di ingegneria sociale

Esempio di ingegneria sociale

01

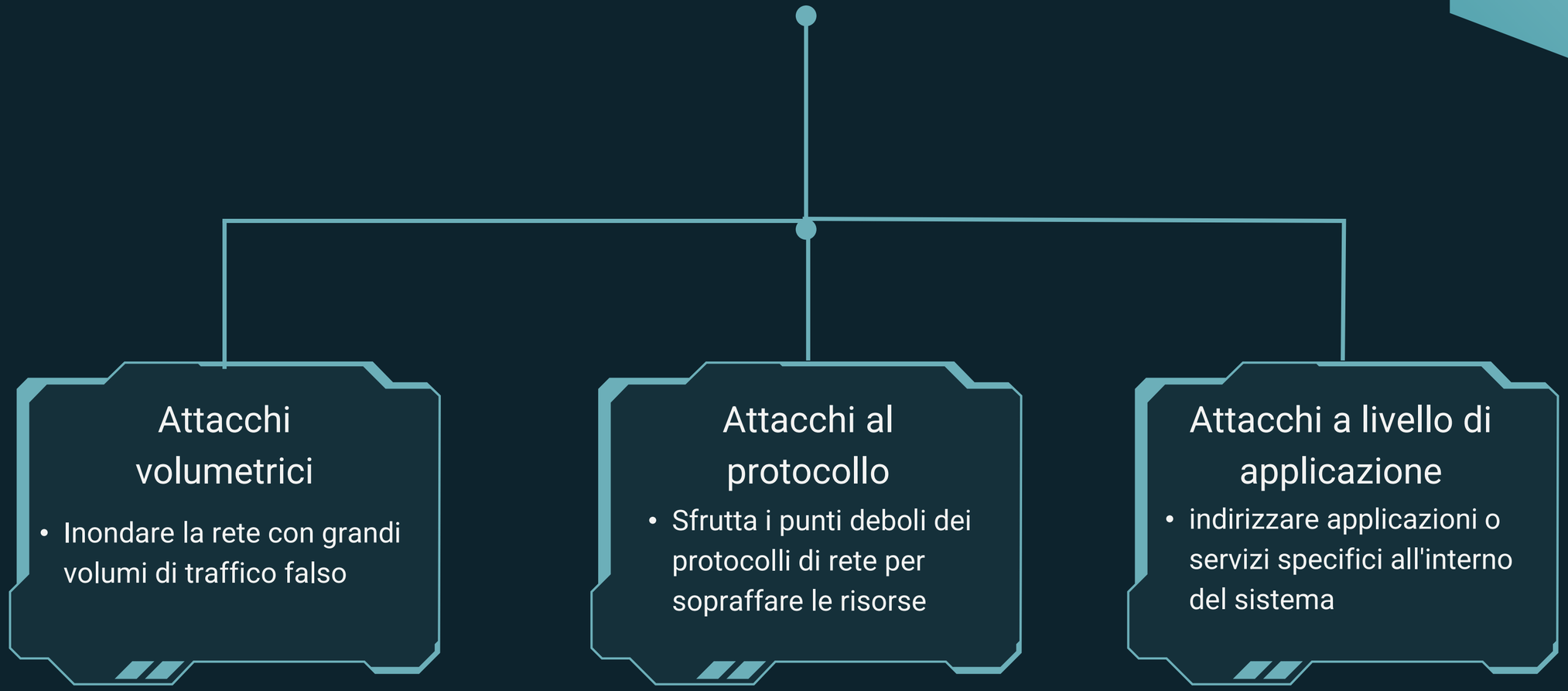
Truffe telefoniche
gli aggressori si spacciano per il supporto tecnico di aziende come Microsoft, IBM o un provider di servizi Internet

- Affermano che il computer della vittima è compromesso e li istruiscono a installare un software di accesso remoto
- Gli aggressori possono installare malware, rubare informazioni o richiedere il pagamento per riparazioni false, > perdite finanziarie, furto di identità, stress emotivo, perdendo anche la fiducia nei servizi di supporto tecnico legittimi

Che cos'è il Distributed Denial of Service (DDoS)?

Che cos'è il Distributed Denial of Service (DDoS)?

L'attacco DDoS utilizza numerosi dispositivi infetti, noti come botnet, per inondare un sistema bersaglio con traffico falso, rendendolo inaccessibile agli utenti legittimi.



Esempio di attacco DDoS

Esempio di attacco DDoS

01

Attacco Dyn (2016)
ha preso di mira il provider DNS Dyn utilizzando una botnet di dispositivi IoT infettati dal malware Mirai, > gravi interruzioni su siti come Twitter, GitHub e Netflix, causando interruzioni di Internet negli Stati Uniti e in Europa per ore

- l'attacco ha messo in luce le vulnerabilità dell'IoT e ha evidenziato il ruolo critico dei provider DNS nella stabilità di Internet, portando a progressi nella sicurezza dell'IoT e nelle strategie di mitigazione degli attacchi DDoS

Che cosa sono le minacce interne?

Che cosa sono le minacce interne?

Le minacce interne sono rischi che hanno origine all'interno di un'organizzazione, in genere coinvolgono dipendenti, ex dipendenti, appaltatori o partner commerciali che hanno accesso a informazioni sensibili.

Insider malintenzionati

- individui che cercano intenzionalmente di danneggiare o rubare informazioni dall'organizzazione

Insider non intenzionali

- individui che inavvertitamente compromettono la sicurezza a causa di negligenza o mancanza di consapevolezza

Esempio di attacco DDoS

Esempio di attacco DDoS

01

Edward Snowden (2013)
un ex appaltatore della NSA ha fatto trapelare documenti top-secret sulla sorveglianza del governo degli Stati Uniti, tra cui la raccolta di metadati e l'accesso ai dati di aziende come Google e Facebook

- ha acceso dibattiti globali sulla privacy, ha spinto le riforme dell'intelligence statunitense e ha sottolineato il grave impatto delle minacce interne, accelerando la spinta verso una crittografia e una sicurezza dei dati più forti

Fatti interessanti sulle minacce informatiche

Fatti interessanti sulle minacce informatiche

Ogni giorno vengono rilevati oltre 350.000 nuovi campioni di malware

Il phishing rimane una delle principali preoccupazioni, con circa il 12% degli utenti che cliccano sui link di phishing.

L'ingegneria sociale è una grave minaccia, che causa dal 70% al 90% delle violazioni dei dati.

Gli attacchi DDoS sono dirompenti, con una durata media di 12 ore

Le minacce interne possono essere costose, con un costo medio degli incidenti di 11,5 milioni di dollari

Esempio di attacco ransomware

Esempio di attacco ransomware

01

Attacco ransomware alla produzione ABC

Un'e-mail di phishing ha causato un attacco ransomware, crittografando i dati critici e interrompendo la produzione per giorni, con conseguente pagamento di un riscatto di $ 50.000

- Key Takeaway: la formazione dei dipendenti sulla consapevolezza del phishing è essenziale per prevenire tali incidenti
- Implementa l'autenticazione a più fattori e backup regolari dei dati per mitigare i rischi

Esempio di attacco interno

Esempio di attacco interno

02

Furto di dati presso XYZ Marketing

Un ex dipendente scontento ha rubato i dati sensibili dei clienti e li ha venduti a un concorrente, causando perdite finanziarie e danni alla reputazione

- sottolinea l'importanza di revocare tempestivamente l'accesso ai dipendenti licenziati
- pone l'accento sull'implementazione dell'accesso ai dati basato sui ruoli e sulla revisione periodica delle policy di sicurezza

Esempio di attacco DDoS

Esempio di attacco DDoS

03

Attacco DDoS a E-Shop Ltd.
Un attacco botnet ha inondato i server del rivenditore, interrompendo le vendite online e danneggiando la fiducia dei clienti

- sottolinea l'importanza di implementare la protezione DDoS e di testare regolarmente la resilienza
- sottolinea la necessità di un'infrastruttura IT scalabile per gestire tali attacchi

Modulo 3: Architettura di sicurezza e misure di protezione

For Small and Medium-Sized Enterprises (SMEs)

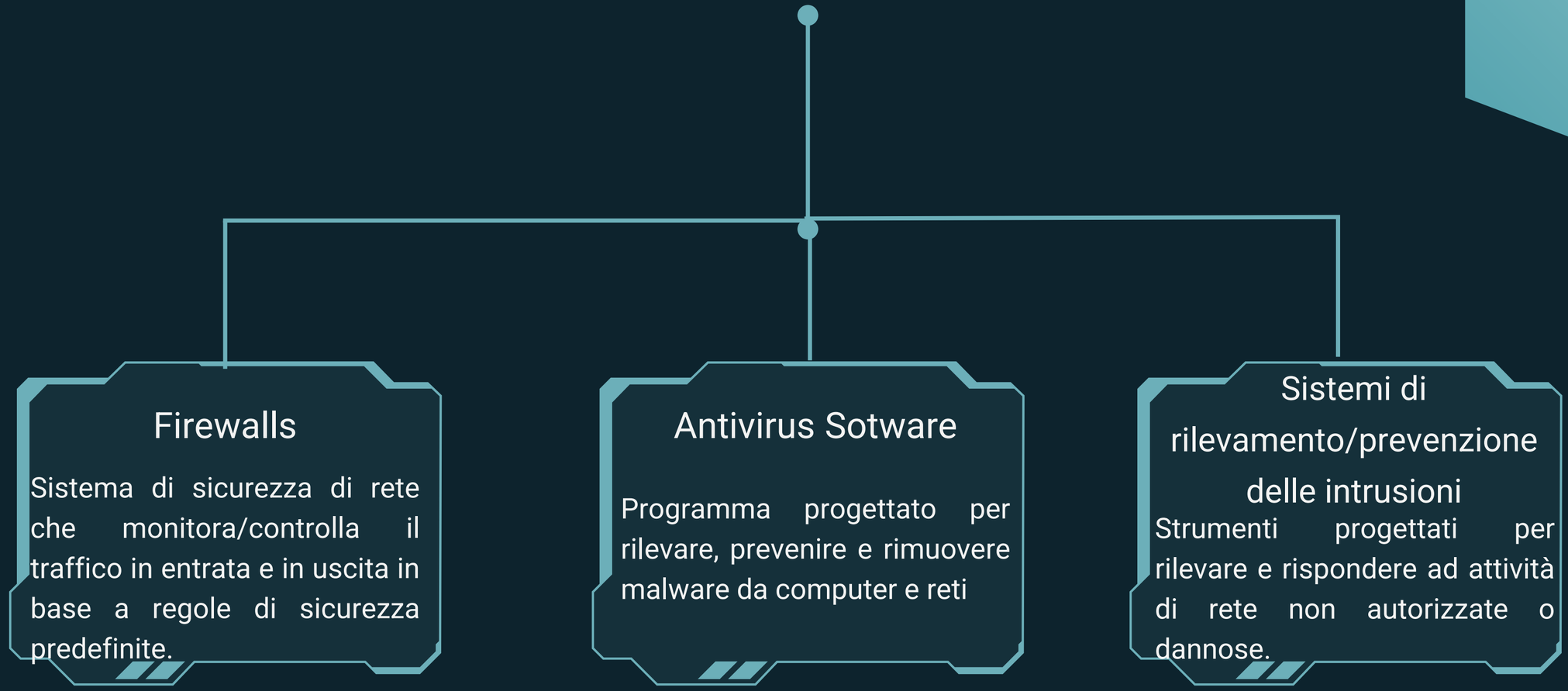
Presenter:
Dr. Tomislav Horvat

University North,
Croatia

Interreg CENTRAL EUROPE
Co-funded by the European Union
COEUS

Architettura di sicurezza

Architettura di sicurezza



Firewalls

Firewalls

01 agiscono come primo livello di difesa creando una barriera tra reti interne affidabili e fonti esterne non attendibili

02 Il ruolo principale è quello di gestire il traffico di rete, garantendo che sia consentito solo l'accesso autorizzato

- Firewall per il filtraggio dei pacchetti
- Stateful Inspection Firewall
- Firewall di nuova generazione (NGFW)

Software Antivirus

Software Antivirus

01

Uno strumento vitale per rilevare e rimuovere malware, inclusi virus, ransomware e spyware.

Rilevamento basato su firma

Rilevamento basato sull'euristica

Sistemi di rilevamento e prevenzione delle intrusioni

Intrusion Detection and Prevention Systems (IDS/IPS)

01 IDS (Intrusion Detection System) monitora il traffico di rete alla ricerca di attività insolite, segnalando potenziali minacce.

02 Gli IPS (Intrusion Prevention System) bloccano le minacce in tempo reale.

Network-Based IDS/IPS

Monitora il traffico attraverso la rete.

Host-Based IDS/IPS

Monitora le attività sui singoli dispositivi.

Backup, Data Recovery and Network Security Management

Backup

Backup

01

Il backup è il processo di creazione di copie dei dati per prevenirne la perdita a causa di guasti hardware, attacchi informatici o cancellazioni accidentali.

Backup completo

Copia completa dei dati.

Backup incrementale

Salva solo le modifiche apportate dall'ultimo backup.

Backup differenziale

Acquisisce le modifiche apportate dall'ultimo backup completo.

02

Regola 3-2-1 - Assicurarsi che i backup siano archiviati su supporti e posizioni diversi (best practice)

Recupero dati

Recupero dati

01 Il recupero dei dati consiste nel ripristinare i dati persi o danneggiati dai backup.

02 Frequenza di backup: secondo una ricerca, il 30% delle persone non ha mai eseguito il backup dei propri dati.

03 Regola 3-2-1: assicurati che i backup siano archiviati su diversi supporti e posizioni (best practice).

Gestione della sicurezza della rete

Gestione della sicurezza della rete

01

La gestione della sicurezza della rete comprende misure per proteggere una rete da accessi non autorizzati e attacchi.

Segmentazione della rete

Divisione di una rete in sezioni isolate per contenere le violazioni.

Encryption

Proteggere i dati in modo che rimangano inaccessibili senza le chiavi di decrittazione appropriate.

VPNs (Virtual Private Networks)

Garantire canali di comunicazione sicuri e crittografati, in particolare per gli utenti remoti.

Access Control Policies

Regolazione dell'accesso degli utenti alle risorse sensibili in base a ruoli e autorizzazioni.

Misure proattive

Misure preventive

01

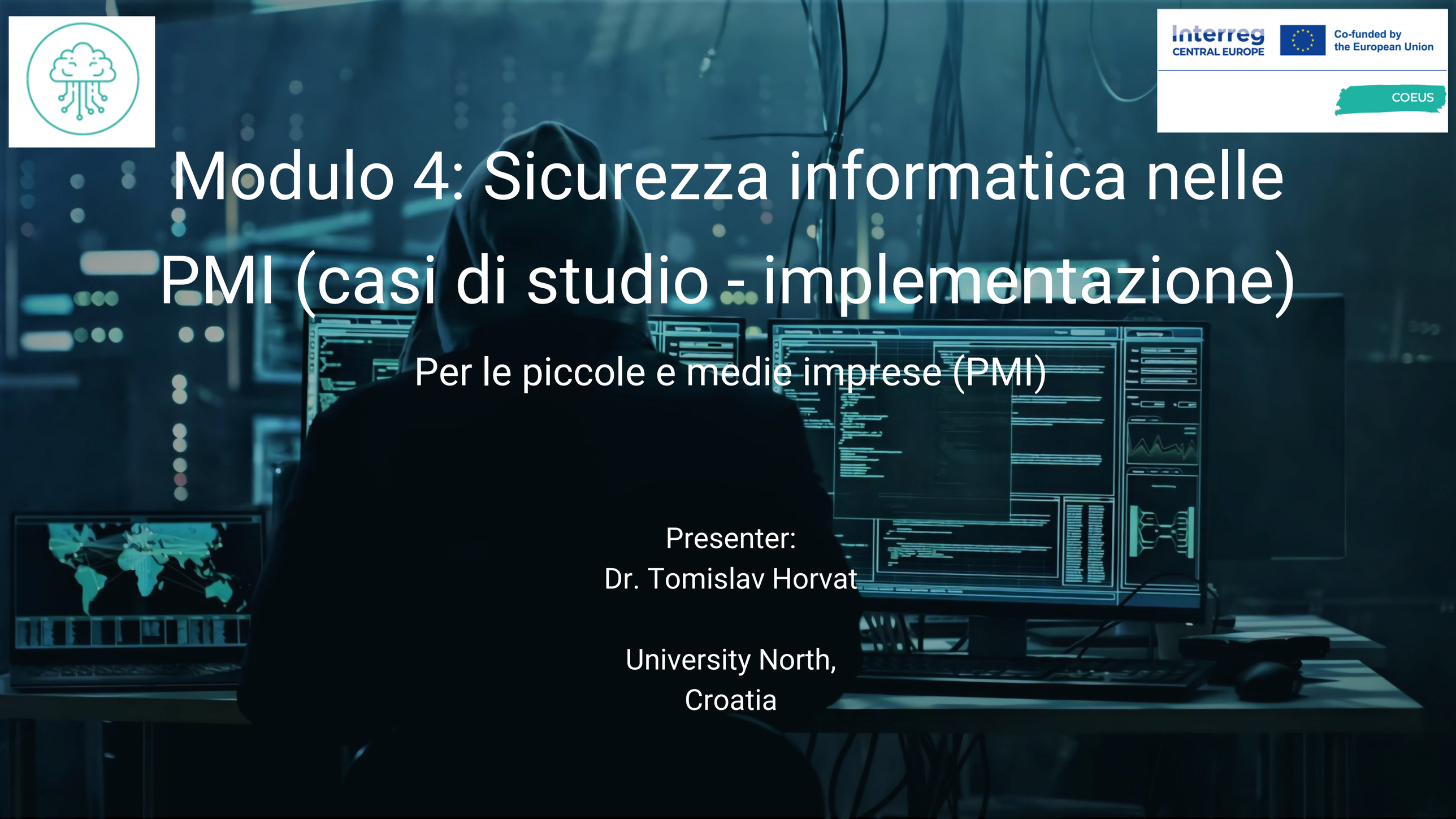
Le misure preventive svolgono un ruolo cruciale nel rafforzare la posizione di sicurezza informatica di un'organizzazione.

Formazione dei dipendenti

Aggiornamenti regolari del sistema e del software

Monitoraggio e analisi dei log

Test del sistema di sicurezza



Modulo 4: Sicurezza informatica nelle PMI (casi di studio - implementazione)

Per le piccole e medie imprese (PMI)

Presenter:
Dr. Tomislav Horvat

University North,
Croatia

Interreg CENTRAL EUROPE
Co-funded by the European Union
COEUS

Panificio SweetBites

Panificio SweetBites

01 Azienda a conduzione familiare con il semplice obiettivo di preparare e vendere torte fatte in casa

02 Man mano che la panetteria cresceva, la famiglia si è espansa online con un sito web, ordini e social media

03 Con l'apertura del negozio, SweetBites ha dovuto affrontare sfide di sicurezza informatica per proteggere i dati dei clienti, il Wi-Fi e i sistemi online

Piano per la Cybersecurity

Piano per la Cybersecurity

01 **Password sicure e accesso utente:** utilizza password complesse e univoche, abilita l'autenticazione a due fattori (2FA) e implementa il controllo degli accessi basato sui ruoli (RBAC)

02 **Proteggi il sito web, il negozio online e il sistema di prenotazione:** implementa un certificato SSL, utilizza un Web Application Firewall (WAF) e aggiorna regolarmente il software

03 **Proteggi la rete e il Wi-Fi pubblico:** utilizza la segmentazione della rete, abilita la crittografia WPA3 e implementa le VLAN per isolare i dati sensibili

04 **Backup e protezione regolari dei dati:** automatizza i backup dei dati, sviluppa un piano di ripristino di emergenza e utilizza la crittografia per proteggere i file di backup

05 **Formare i dipendenti e monitorare continuamente la sicurezza:** condurre regolarmente corsi di formazione sulla sicurezza informatica, eseguire simulazioni di phishing e utilizzare strumenti di monitoraggio continuo per rilevare le minacce

TechRise Solutions

TechRise Solutions

01

TechRise Solutions, una piccola azienda a conduzione familiare, ha iniziato in un garage fornendo software personalizzato ai clienti locali con una configurazione di rete di base.

02

Con la crescita, TechRise ha assunto dipendenti e adottato l'infrastruttura cloud, introducendo vulnerabilità nei dati dei clienti e nella sicurezza del cloud.

03

Con 50 dipendenti, molti dei quali da remoto, la sicurezza informatica è diventata più complessa, richiedendo un lavoro remoto sicuro, conformità alle normative e difesa contro le minacce avanzate.

04

TechRise è cresciuta da un'azienda locale a un'azienda tecnologica nazionale, che richiede una solida sicurezza informatica per proteggere il cloud, le applicazioni e le risorse digitali.

Piano per la Cybersecurity

Piano per la Cybersecurity

01 **Rafforza le password e i controlli di accesso:** utilizza password complesse, MFA e RBAC per prevenire accessi non autorizzati e attacchi con password

02 **Proteggi le applicazioni cloud e web:** crittografa i dati, utilizza i WAF, implementa SSL e conduci controlli di sicurezza regolari

03 **Proteggi il lavoro remoto:** utilizza VPN, soluzioni EDR e MDM per proteggere i dispositivi e le connessioni remote

04 **Implementa backup e ripristino di emergenza -** Automatizza i backup, crea un DRP e utilizza backup immutabili per ripristinare rapidamente i dati

05 **Monitorare i sistemi e formare i dipendenti:** fornire formazione regolare, monitorare i sistemi con strumenti SIEM ed eseguire simulazioni di phishing