SEGRETI AZIENDALI E CONCORRENZA SLEALE

Strumenti di prova a disposizione del management

Martedì 03 dicembre 2024

Ore 16:00 – 18:00

Convegno online

CONSIGLIO NAZIONALE DEGLI INGEGNERI

Prof. a.c. Michele Vitiello

Dottore in Ingegneria delle Telecomunicazioni

Professore a.c. Università Telematica Internazionale UNINETTUNO
Consulente della Direzione Investigativa e Distrettuale Antimafia (DIA, DDA)
Docente della Scuola Superiore della Magistratura
Titolare dello Studio Ingegneria Informatica Forense con sede a Brescia
Consigliere all'Ordine degli Ingegneri di Brescia
Iscritto all' Albo Nazionale dei Periti e CTU
Consulente Tecnico per n°90 Uffici Giudiziari, di cui n°55 Procure della Repubblica, n° 35 Tribunali e n°3 Procure Estere
Ha svolto oltre n°3.000 consulenze tecniche e perizie forensi
Vincitore Investigation & Forensic Awards 2022 - premio Eccellenza dell' Informatica e Telefonia Forense
Opinionista Esperto Scientifico ORE 14 Rai 2, Uno mattina Rai 1 e Italia sotto inchiesta Rai Radio 1, Quarto Grado Rete 4

Obiettivi del convegno

Aggiornamento Professionale

Fornire ai partecipanti le ultime conoscenze su metodi di prevenzione e strategie di sicurezza aziendale.

Valutazione del Rischio

Permettere al management di effettuare valutazioni consapevoli sui rischi di concorrenza sleale.

Pianificazione Strategica

Facilitare lo sviluppo di piani e programmi d'azione per proteggere i segreti aziendali.

A chi è rivolto il convegno

Ingegneri Civili

Professionisti specializzati in progettazione e costruzione di infrastrutture.

Ingegneri Ambientali

Esperti in soluzioni sostenibili e gestione delle risorse naturali.

Ingegneri Gestionali

Specialisti in ottimizzazione dei processi aziendali e gestione delle risorse.

Figure Tecniche

Professionisti operanti nell'ingegneria economica e gestionale.

Argomenti principali

1

Dipendente infedele

Approfondimento sulla figura del dipendente infedele e sulle modalità di furto di dati aziendali.

2

Digital Forensics nella protezione dei segreti aziendali

Introduzione al ruolo cruciale della digital forensics nell'era digitale per la salvaguardia delle informazioni riservate e dei segreti aziendali.

3

Digital Forensics come prova legale

Analisi dell'applicabilità e dell'importanza delle evidenze digitali nei procedimenti legali relativi alla concorrenza sleale.

4

Prevenzione e strategie di sicurezza

Discussione sulle migliori pratiche e strategie per prevenire la fuga di informazioni sensibili e proteggere l'azienda dalla concorrenza sleale.

Il Dipendente Infedele: un rischio interno

Caratteristiche

Il dipendente infedele, spesso insoddisfatto verso l'azienda, i titolari o i colleghi, rappresenta una minaccia interna sfruttando la conoscenza delle vulnerabilità aziendali. Utilizza tecniche come il social engineering per manipolare colleghi, il dumpster diving per recuperare documenti sensibili dai rifiuti e il tailgating per accedere ad aree riservate. Queste azioni possono portare alla sottrazione di dati riservati, causando danni economici e reputazionali all’organizzazione.

Motivazioni

Gli scopi della sottrazione di informazioni includono la vendita di dati sensibili a competitor per vantaggi economici, l’avvio di attività concorrenti violando patti di non concorrenza, l’estorsione per ottenere denaro o favori e il danneggiamento dell’immagine aziendale attraverso la diffusione di informazioni riservate, con gravi conseguenze economiche e reputazionali.

Metodi di sottrazione di informazioni

Social engineering

Tecniche di manipolazione psicologica per ottenere accesso non autorizzato a informazioni riservate.

Dumpster Diving

Ricerca di informazioni sensibili tra i rifiuti aziendali o nelle scrivanie non sorvegliate.

Tailgating

Accesso non autorizzato ad aree riservate seguendo dipendenti autorizzati.

Backup non autorizzati

Copia di dati aziendali su dispositivi personali o cloud non controllati.

Accesso non autorizzato ai sistemi

Elevazione dei privilegi

Il dipendente infedele cerca di ottenere permessi di amministratore per accedere a dati e aree riservate.

Utilizzo di credenziali o dispositivi altrui

Sfrutta dispositi altrui e password rubate o condivise per mascherare la propria identità durante l'accesso.

Bypass dei controlli di sicurezza

Tenta di aggirare firewall e sistemi di rilevamento delle intrusioni per accedere a risorse protette.

Strumenti per l’esfiltrazione dei dati

Dispositivi USB

Pendrive e hard disk USB utilizzati per copiare rapidamente grandi quantità di dati.

Servizi cloud

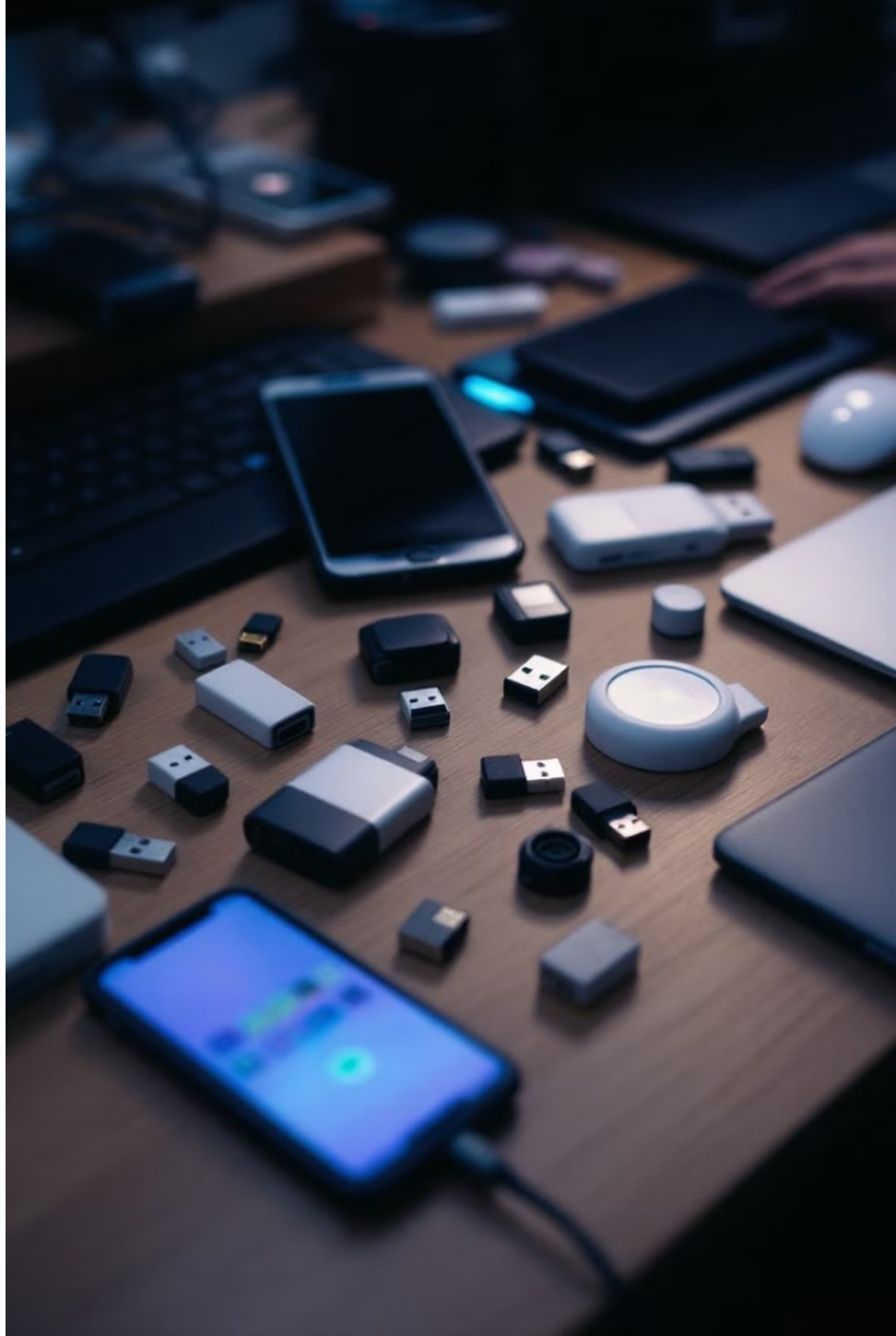
Impiegati per trasferire dati su account personali esterni all'azienda, come ad esempio Google Drive, Dropbox, OneDrive.

Email personali

Usate per inviare informazioni sensibili a indirizzi esterni non monitorati.

Dispositivi mobili

Sfruttati per fotografare schermi o documenti fisici contenenti dati riservati.



Tecniche di occultamento delle attività

Cancellazione dei Log

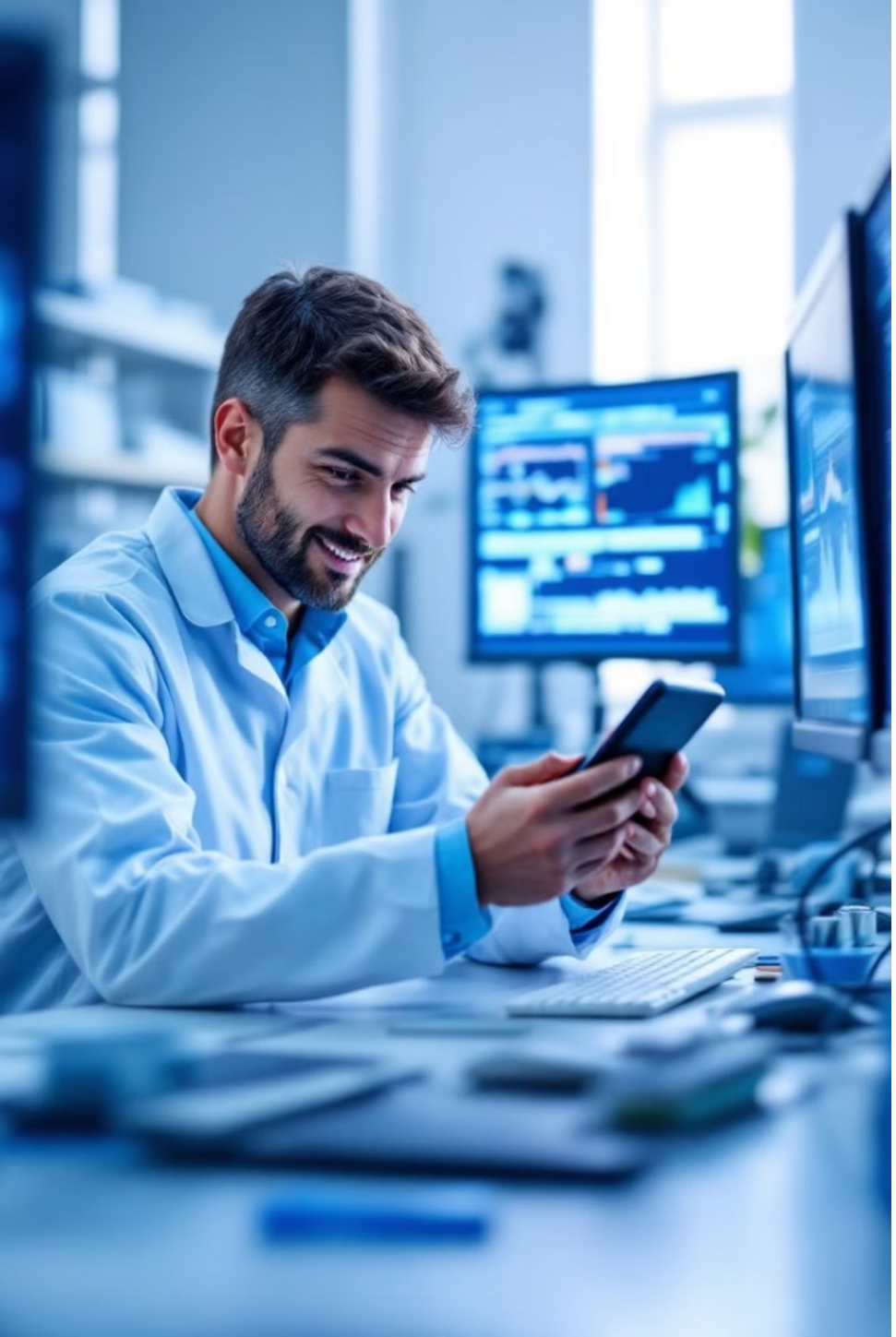
Il dipendente infedele tenta di eliminare o modificare i log di sistema per nascondere le proprie azioni. Questo può includere la manipolazione dei file di registro, l'uso di strumenti di pulizia del disco o l'alterazione delle impostazioni di logging.

Uso di VPN e proxy

Per mascherare la propria identità e localizzazione, il malintenzionato potrebbe utilizzare reti private virtuali (VPN) o server proxy. Queste tecnologie rendono più difficile tracciare l'origine delle attività sospette.

Crittografia dei dati rubati

Per evitare che i dati sottratti vengano facilmente identificati, il dipendente potrebbe crittografarli o modificarne l’estensione prima dell'esfiltrazione. Questo rende più complessa l'analisi del contenuto in caso di intercettazione.



Il ruolo della Digital Forensics

1

Acquisizione dei dati

Raccolta di prove digitali nel rispetto delle normative vigenti, generando le copie forensi dei dispositivi e degli account cloud di interesse.

2

Analisi dei dispositivi

Esame forense di PC, smartphone, USB, account cloud e altri supporti digitali, previa operazione di indicizzazione dati mediante software forensi.

3

Ricostruzione Timeline

Creazione di una cronologia dettagliata degli eventi, utile a ricostruire le azioni malevole messe in campo dal dipendente infedele.

4

Relazione tecnica

Produzione di resoconti validi in ambito giudiziario, come ad esempio la Relazione Tecnica ben dettagliata e specifica.

Doveri dell’informatico forense

Consulenza e verifica preliminare

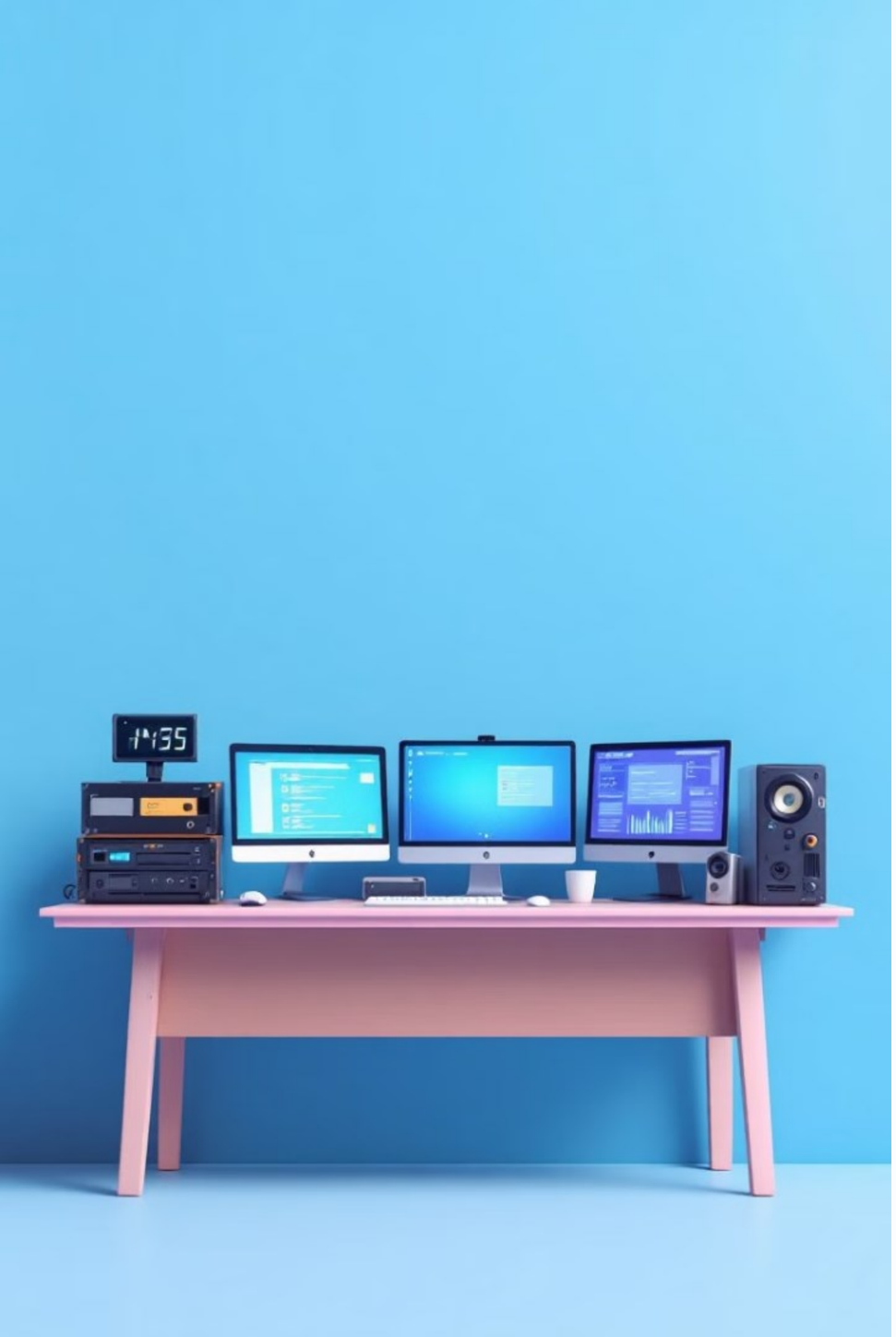
Il professionista, dopo una prima fase di verifica, consiglia il cliente sui passaggi da seguire.

Operazioni tecniche di copia forense

Vengono generate le copie forensi delle evidenze di possible interesse nel rispetto delle best practices della disciplina.

Analisi dei dati e stesura della relazione

Il consulente, previa comprensione del contesto, analizza le evidenze informatiche al fine di certificare il furto di dati e l’accesso non autorizzato da parte del dipendente infedele.



Kit dell’esperto di Digital Forensics: strumenti essenziali per indagini

Hardware specializzato

Write blockers, dispositivi di clonazione forense, adattatori per vari tipi di storage.

Software di analisi

Cellebrite, FTK, Autopsy, Axiom, per l'analisi approfondita dei dati.

Strumenti di recupero dati

Software per il recupero di dati cancellati o danneggiati.

Strumenti vari

Fotocamere ad alta risoluzione, set di cacchiaviti e quant’altro utile.

Gli strumenti essenziali per un consulente informatico forense includono dispositivi per effettuare copie forensi (duplicatori forensi, write blocker, software specifici e distribuzioni Linux digital forensics), write blocker, software specializzati in mobile e cloud forensics come Cellebrite, Oxygen e Magnet. È importante descrivere mediante apposito verbale ogni operazione compiuta, calcolare i valori HASH delle copie forensi, al fine di certificare i dati come fonti di prova valide.

Esame delle evidenze

Analisi forense delle evidenze

Si effettua la copia forense di hdd e dispositivi mobile per esaminare file cancellati, frammenti di dati e metadati. Questo permette di recuperare informazioni anche se apparentemente eliminate.

Ispezione dei dispositivi rimovibili

Si analizzano USB drive, schede SD e altri supporti rimovibili, ove individuati, per tracciare il movimento dei dati. Si cercano evidenze di copie non autorizzate o trasferimenti sospetti.

Verifica dei backup e dati su NAS e Server

Si esaminano i backup aziendali, oltre ai dati su NAS e server, per identificare discrepanze o manipolazioni nei dati storici, che potrebbero indicare tentativi di coprire le tracce.

Analisi delle impronte digitali dei file

Si utilizzano tecniche di hashing per verificare l'integrità dei file e identificare eventuali modifiche non autorizzate ai dati aziendali.

Analisi del traffico di rete

1

Monitoraggio dei flussi di dati

L'informatico forense analizza i log di rete, ove registrati, per identificare trasferimenti di dati insoliti o di grandi dimensioni verso destinazioni esterne.

2

Rilevamento di connessioni sospette

Si cercano connessioni a indirizzi IP non autorizzati o a servizi cloud personali non approvati dall'azienda.

3

Analisi dei protocolli

Si esaminano i protocolli di comunicazione utilizzati per identificare l'uso di tecniche di tunneling o di crittografia non standard.

4

Correlazione temporale

Si mettono in relazione le attività di rete sospette con gli orari di lavoro e le responsabilità del dipendente.

Tecniche di recovery dei dati eliminati

1

Scansione dei settori non allocati

Ricerca di frammenti di dati in aree del disco apparentemente vuote.

2

Analisi dei File System

Esame delle strutture di file system per recuperare file cancellati.

3

Carving dei dati

Ricostruzione di file basata su firme e strutture note.

4

Recupero da backup e snapshot

Estrazione di dati da copie di sicurezza e istantanee del sistema.

Il recupero dei dati eliminati è fondamentale per scoprire tentativi di occultamento. Queste tecniche permettono di riportare alla luce informazioni che il dipendente infedele potrebbe aver cercato di distruggere, fornendo prove cruciali per l'indagine.

La Descrizione Informatica: strumento legale

Definizione

Provvedimento giudiziario d'urgenza per raccogliere prove di violazioni di diritti di proprietà industriale, diritto d'autore e diritti del lavoro.

Scopo

Individuare, acquisire e conservare dati sensibili per sostenere richieste di risarcimento o azioni legali.

Normativa

Regolata dagli articoli 129 e 130 del Codice della Proprietà Industriale.

Requisiti per la Descrizione Informatica

Fumus Boni Iuris

Evidenza sufficiente di un diritto violato, dimostrando la probabilità di successo dell'azione legale.

Periculum in Mora

Urgenza dell'intervento per evitare danni irreparabili, giustificando l'azione immediata.

Procedura Inaudita Altera Parte

Spesso attuata senza preavviso alla controparte per preservare l'effetto sorpresa e l'integrità delle prove.

Fasi operative della Descrizione Informatica

1

Identificazione

Isolamento dei sistemi, dei dispositivi informatici e degli account rilevanti

2

Acquisizione

Creazione di doppia copia forense dei dati, al fine di rispondere ai quesiti posti dal Giudice competente

3

Documentazione

Compilazione dettagliata del verbale operative in collaborazione con Ufficiale Giudiziario

4

Conservazione

Custodia sicura dei dati per analisi future

La fase operativa richiede precisione e metodologia rigorosa per garantire la validità legale delle prove raccolte e preservare l'integrità dei dati acquisiti.

Procedimenti giudiziari e digital forensics: valore probatore dei risultati

Requisiti legali

I risultati delle indagini forensi devono rispettare rigorosi standard legali per essere ammissibili in tribunale. Ciò include la documentazione dettagliata di ogni fase dell'indagine, la preservazione della catena di custodia e l'utilizzo di strumenti e metodi forensi riconosciuti.

Presentazione delle prove

Le prove digitali devono essere presentate in modo chiaro e comprensibile per il giudice. Questo spesso richiede l'uso di visualizzazioni grafiche e spiegazioni dettagliate da parte di esperti forensi. La capacità di spiegare concetti tecnici complessi in termini semplici è cruciale.

Il valore probatorio dei risultati di digital forensics nei procedimenti giudiziari dipende dalla qualità e dall'integrità delle indagini condotte. È fondamentale seguire procedure rigorose e documentate per garantire che le prove digitali siano ammissibili e convincenti in tribunale.

La Formazione dei dipendenti come prima linea di difesa

1. ## Sensibilizzazione iniziale

   Introdurre i concetti base di sicurezza informatica a tutti i nuovi dipendenti durante l'onboarding.

2. ## Formazione continua

   Organizzare corsi regolari per aggiornare le competenze e informare sulle nuove minacce.

3. ## Simulazioni pratiche

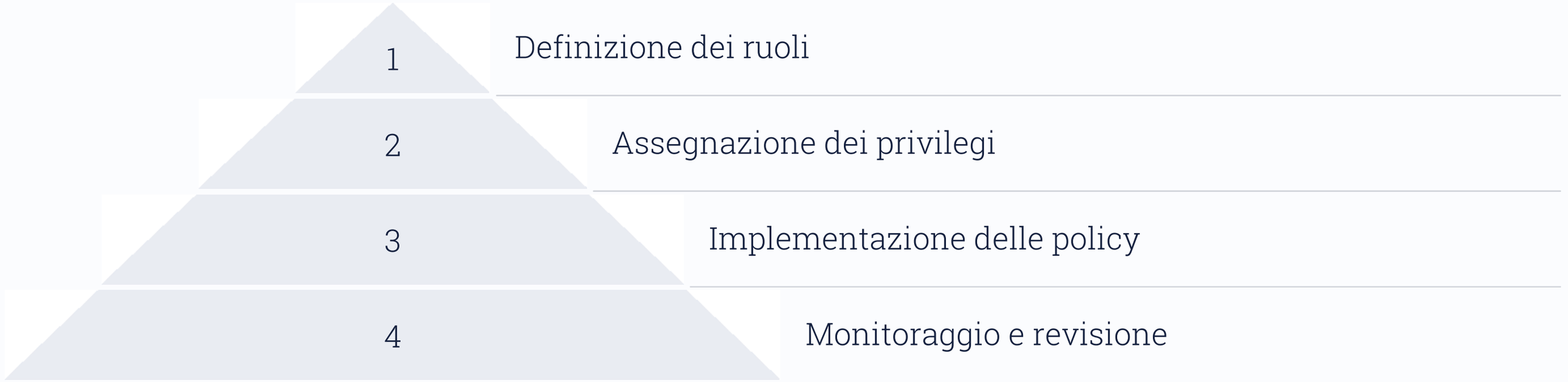
   Condurre esercitazioni di phishing e altri scenari di attacco per testare la prontezza dei dipendenti.

4. ## Valutazione e miglioramento

   Analizzare i risultati delle formazioni e delle simulazioni per migliorare costantemente il programma.

La formazione dei dipendenti è cruciale per creare una cultura aziendale di sicurezza. Dipendenti ben informati e consapevoli rappresentano la prima e più efficace linea di difesa contro le minacce informatiche. Una formazione efficace non solo riduce i rischi di incidenti, ma promuove anche un senso di responsabilità condivisa per la sicurezza aziendale.

Policy aziendali per la protezione dei dati: ruoli e privilegi



La creazione di policy efficaci per la protezione dei dati è fondamentale per minimizzare i rischi. Inizia con una chiara definizione dei ruoli all'interno dell'organizzazione, seguita da un'attenta assegnazione dei privilegi di accesso. L'implementazione delle policy deve essere accompagnata da un costante monitoraggio e da revisioni periodiche per adattarsi alle nuove minacce.

È essenziale che ogni dipendente comprenda il proprio ruolo nella protezione dei dati e le responsabilità associate. Le policy devono essere chiare, facilmente accessibili e regolarmente aggiornate per riflettere i cambiamenti nel panorama della sicurezza informatica.

Integrità, disponibilità e confidenzialità: pilastri della sicurezza informatica

Confidenzialità

Garantisce che solo le persone autorizzate possano accedere ai dati sensibili.

Integrità

Assicura che i dati non vengano alterati o manipolati senza autorizzazione.

Disponibilità

Garantisce che i dati siano accessibili quando necessario agli utenti autorizzati.

Questi tre principi fondamentali costituiscono la base per una gestione sicura dei dati. La confidenzialità protegge le informazioni sensibili da accessi non autorizzati. L'integrità garantisce l'accuratezza e la completezza dei dati nel tempo. La disponibilità assicura che i sistemi e i dati siano accessibili quando necessario, bilanciando sicurezza e funzionalità.

L'implementazione di questi principi richiede una combinazione di misure tecniche, come crittografia e controlli di accesso, e pratiche organizzative, come la formazione del personale e la gestione dei rischi.

Best Practices aziendali

24/7

Monitoraggio continuo

Implementare sistemi di sorveglianza della rete e delle attività degli utenti attivi 24 ore su 24, 7 giorni su 7.

256

Crittografia avanzata

Utilizzare algoritmi di crittografia a 256 bit per proteggere i dati sensibili sia in transito che a riposo.

2FA

Autenticazione a due fattori

Imporre l'uso dell'autenticazione a due fattori per tutti gli accessi ai sistemi critici.

90%

Formazione del personale

Assicurarsi che almeno il 90% del personale riceva una formazione regolare sulla sicurezza informatica.

La prevenzione e il rilevamento tempestivo sono fondamentali per contrastare le minacce interne. Implementando queste best practices e mantenendo un approccio proattivo alla sicurezza, le aziende possono significativamente ridurre il rischio di furto di dati da parte di dipendenti infedeli.

Grazie per l'attenzione

Prof. a.c. Michele Vitiello
Studio Ingegneria Informatica Forense

Via Cefalonia, 70 Brescia (BS)
Tel: 0303540238 – Cell. 347.1527252
Mail: info@michelevitiello.it web: www.michelevitiello.it