UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale

Agenzia per la Coesione Territoriale

Presidenza del Consiglio dei Ministri
Dipartimento della Funzione Pubblica

PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020

Competenze digitali per la PA

Proteggere i dispositivi

Corrado Giustozzi

FormezPA

Temi chiave del modulo

Livello Base	Livello Intermedio	Livello Avanzato
Conoscere l'esistenza di rischi e minacce negli ambienti digitali	Saper valutare i principali rischi per il dispositivo se soggetto ad attacchi informatici	Sapere quali contromisure adottare per prevenire e difendersi dagli attacchi informatici
Saper adottare le misure base di sicurezza per proteggere i dispositivi	Conoscere l'esistenza delle misure minime di sicurezza ICT per le pubbliche amministrazioni	Saper riconoscere quando il dispositivo è soggetto ad attacchi informatici
Saper definire e gestire le password in modo consapevole e protetto	Conoscere i principali tipi di attacco informatico, Virus, Trojan, Denial of Service (DoS), Distributed Denial of Service (DDoS)	

Sommario

- Cosa dobbiamo proteggere (e perché)
- Il contesto e la minaccia
- Le contromisure di protezione
  - il caso delle password
- Le misure minime di sicurezza ICT per la Pubblica Amministrazione

Cosa dobbiamo proteggere?

Il bene supremo della società

- La nostra è la “società dell’informazione”
- L’informazione “tradizionale” è:
  - materiale e coincidente col suo supporto fisico
  - facilmente proteggibile con mezzi fisici
- L’informazione “moderna” è:
  - immateriale e svincolata dal suo supporto fisico
  - difficilmente proteggibile con metodi tradizionali
- L’informazione digitale può facilmente essere:
  - intercettata, copiata, trasportata, spostata, diffusa
  - modificata, contraffatta, falsificata, alterata
  - distrutta

Ubiquità dell'informazione

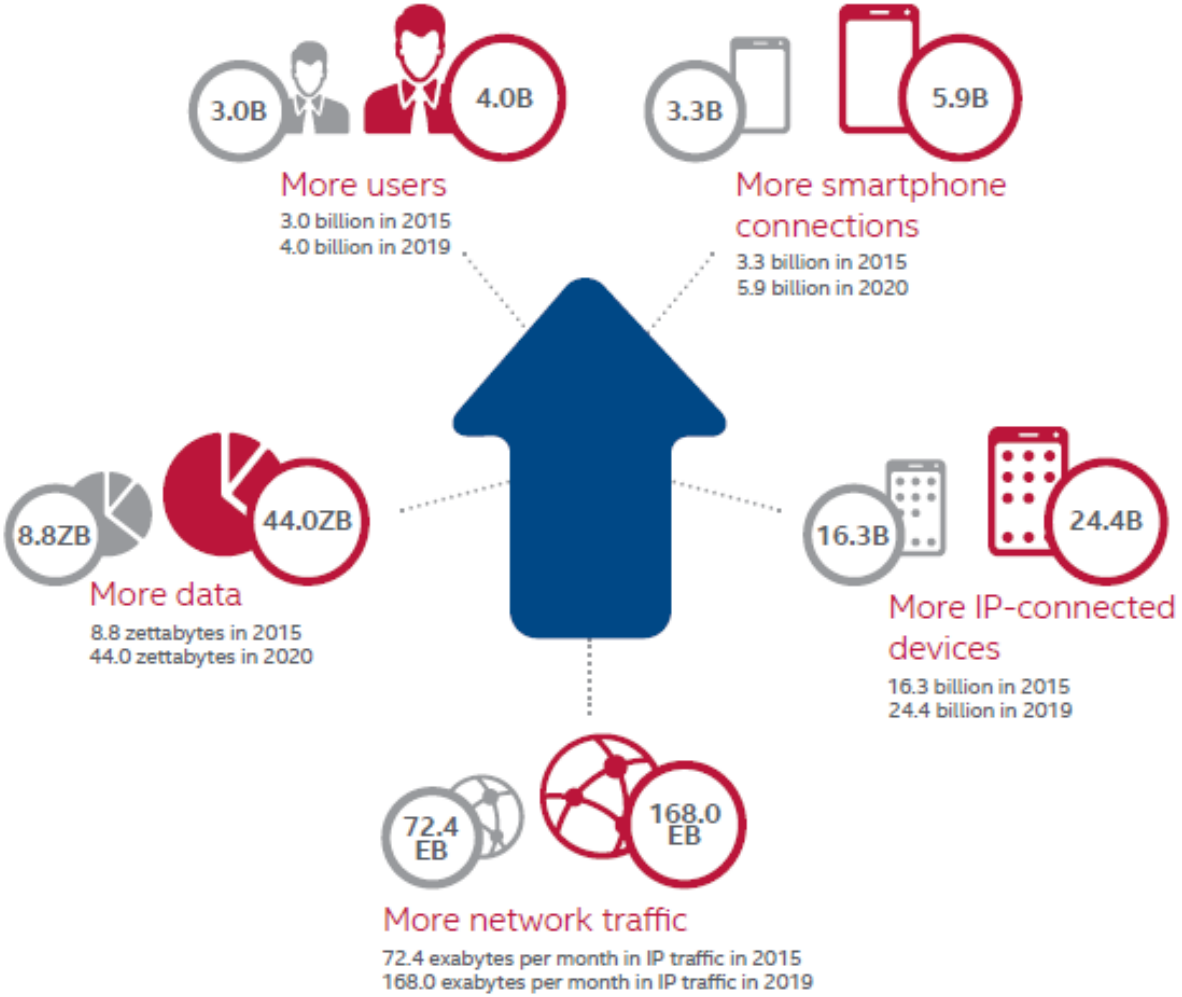
- Oggi la maggior parte delle informazioni di valore viene elaborata ed archiviata su sistemi informativi, personali o non, connessi tra loro in modo sempre meno estemporaneo e sempre più integrato grazie alla crescente pervasività delle reti
- Gli apparati hanno assunto una dimensione personale (smartphone, smartwatch, …), con grande capacità di integrazione di reti diverse (Bluetooth, Wi-Fi, NFC, …)
- La convergenza fra informatica e telefonia ha reso comune anche l'utilizzo delle reti cellulari (GSM, GPRS, UMTS, 4G, 5G, …) per il trasporto di dati e informazioni multimediali integrate
- L'utilizzo promiscuo dei dispositivi (sfera lavorativa/personale) è sempre più comune

Le proprietà fondamentali

- Riservatezza:
  - avere la certezza che una certa informazione possa essere conosciuta solo da chi ha il diritto a farlo
- Integrità:
  - avere la certezza che una certa informazione possa essere modificata solo da chi ha diritto a farlo e solo attraverso modalità note e verificabili
- Disponibilità:
  - avere la certezza che una certa informazione possa essere prontamente reperita ed utilizzata tutte le volte che si ha necessità di farlo

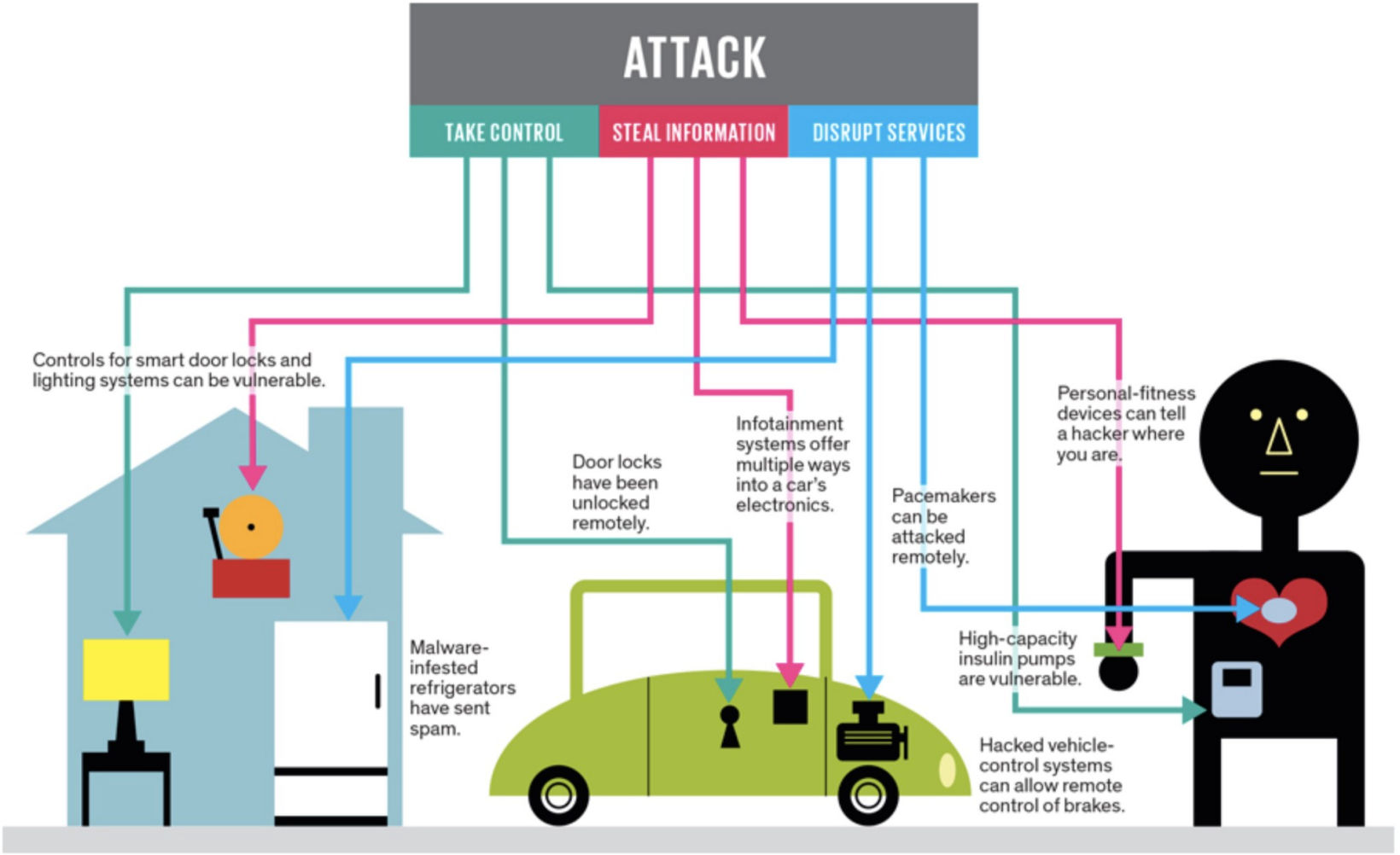
Il contesto e la minaccia

Aumento della superficie d'attacco



Fonte: McAfee Labs, 2015

Tutto è vulnerabile! (Oggetti “smart”)



Le debolezze del sistema

- Debolezze tecniche:
  - insecurity by design: autenticazione debole, messaggi in chiaro, dati memorizzati in chiaro, …
  - errori di progetto: protocolli difettosi, algoritmi inadeguati, …
  - errori di implementazione: bug, codici insicuri, …
- Debolezze date dalla complessità:
  - la complessità dei sistemi e delle reti è sempre più elevata
  - in Rete ci sono semplicemente troppi utenti e dispositivi!
  - il volume di traffico sta diventando ingestibile
- Debolezze del fattore umano e comportamentale:
  - scarsa consapevolezza e cultura da parte dell'utente finale
  - errata percezione dei rischi delle azioni nel ciberspazio
  - l'assunzione fondamentale è che tutti siano in buona fede

Da cosa ci si deve difendere

- Minacce esterne:
  - terzi estranei, curiosi od ostili
  - concorrenti sleali
  - organizzazioni criminali
  - hacker, cyberterroristi, tecnovandali, attivisti, ...
- Minacce interne:
  - errore, incuria, disattenzione, approssimazione, …
  - dipendenti infedeli, insoddisfatti, vendicativi, ...
  - dipendenti curiosi, smanettoni, “furbi”, …
  - personale esterno (consulenti, clienti, fornitori, …)
- Minacce collaterali:
  - triangolazioni

Il quadro dell'attacco

- Gli strumenti:
  - malware (virus, worm, trojan, …)
  - password cracker
- Le modalità di diffusione:
  - phishing
  - spearphishing
- Gli effetti:
  - spionaggio, esfiltrazione di dati
  - sabotaggio, danneggiamento, blocco di servizi
  - truffe verso la persona o l'organizzazione (CEO fraud, …)
  - estorsioni (ransomware, …)
- La vulnerabilità principale:
  - l'essere umano!

Le contromisure

Non solo tecnologia

- La sicurezza delle informazioni si fa a livello:
  - fisico
  - logico
  - organizzativo
- La sicurezza delle informazioni riguarda:
  - dispositivi
  - informazioni
  - processi
  - persone

Classi di contromisure

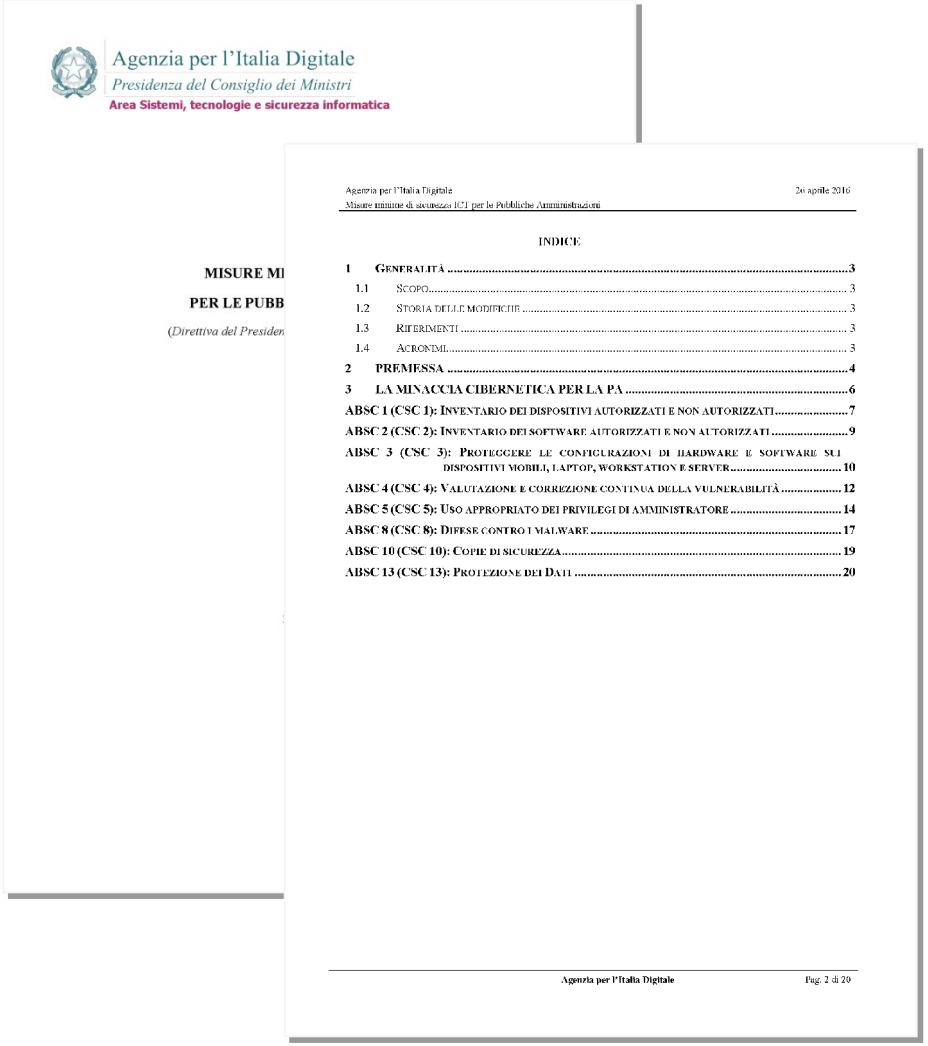
- Fidarsi è bene ma non fidarsi è meglio!
  - insospettirsi in caso di mail, situazioni, eventi anomali o imprevisti
- Corretta custodia e impiego:
  - dei dispositivi (personali, di lavoro)
  - delle credenziali (password, smart card, …)
- Prudente comportamento:
  - accortezze durante la navigazione (https, verifica autenticità, …)
  - uso consapevole dei social network (informazioni personali, truffe)
  - corretto uso di connessioni pubbliche e memorie esterne altrui
  - non scaricare o installare app e software non verificati
- Tecnologie a supporto:
  - antivirus (anche e soprattutto sui cellulari!)
  - crittografia

Le password

- Sono la prima e spesso l'unica tutela che abbiamo
- La grande maggioranza degli attacchi avviene perché l'attaccante viene a conoscenza della password della vittima:
  - scoprendola (password lasciata in evidenza e/o in chiaro)
  - indovinandola (password legata ad informazioni note dell'utente)
  - ricostruendola (password troppo corta e troppo semplice)
  - trafugandola (password utilizzata su un altro servizio compromesso)
- Le regole di comportamento servono ad evitare che ciò accada:
  - **mai** usare la stessa password per più servizi e/o account diversi
  - evitare di usare riferimenti personali e/o parole di senso compiuto
  - sceglierle piuttosto lunghe (almeno otto caratteri)
  - aggiungere cifre e caratteri speciali (meglio se non all'inizio o alla fine)
  - cambiarle periodicamente

Le misure minime di sicurezza ICT per le Pubbliche Amministrazioni

Cronologia e riferimenti normativi


Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri
Area Sistemi, tecnologie e sicurezza informatica

MISURE MI
PER LE PUBB
(Direttiva del Presiden

Agenzia per l'Italia Digitale — 2o aprile 2016
Misure minime di sicurezza ICT per le Pubbliche Amministrazioni

INDICE

Agenzia per l'Italia Digitale — Pag. 2 di 20

- Già anticipate via Web sin da settembre 2016
- Emesse con circolare 18 aprile 2017, n. 2/2017
- Pubblicate in Gazzetta Ufficiale (SG) n.103 del 5/5/2017
- Adozione obbligatoria entro il 31/12/2017
- Dovere d'ufficio del Dirigente responsabile IT (art. 17 CAD)

Obiettivi - 1

- Indirizzare l’esigenza delle Amministrazioni fornendo loro, in particolare a quelle meno preparate, un riferimento operativo direttamente utilizzabile (checklist) nell’attesa della pubblicazione di documenti di indirizzo di più ampio respiro
- Stabilire una baseline comune di misure tecniche ed organizzative irrinunciabili

Obiettivi - 2

- Fornire alle Amministrazioni uno strumento per poter verificare lo stato corrente di attuazione delle misure di protezione contro le minacce informatiche, e poter tracciare un percorso di miglioramento
- Responsabilizzare le Amministrazioni sulla necessità di migliorare e mantenere adeguato il proprio livello di protezione cibernetica ponendo il compito (e la relativa responsabilità) direttamente in capo al dirigente competente

Considerazioni ispiratrici

- Non reinventare la ruota ma basarsi su esperienze consolidate (SANS 20 / CSC)
- Indirizzare le caratteristiche e le esigenze specifiche delle nostre Pubbliche Amministrazioni
- Minimizzare gli impatti implementativi (*effort*, costi)
- Fornire requisiti in linea con le più diffuse e consolidate *best practice* di settore
- Armonizzare il quadro a valle del GDPR e della direttiva NIS

Le famiglie di controlli

- **ABSC 1**: inventario dei dispositivi autorizzati e non autorizzati
- **ABSC 2**: inventario dei software autorizzati e non autorizzati
- **ABSC 3**: proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server
- **ABSC 4**: valutazione e correzione continua della vulnerabilità
- **ABSC 5**: uso appropriato dei privilegi di amministratore
- **ABSC 8**: difese contro i malware
- **ABSC 10**: copie di sicurezza
- **ABSC 13**: protezione dei dati

I livelli di applicazione

- **Minimo**: è quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme
- **Standard**: può essere assunto come base di riferimento nella maggior parte dei casi
- **Avanzato**: deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni

Le modalità di applicazione

- Il raggiungimento di elevati livelli di sicurezza, quando è molto elevata la complessità della struttura e l'eterogeneità dei servizi erogati, può essere eccessivamente oneroso se applicato in modo generalizzato
- Pertanto **ogni Amministrazione dovrà avere cura di individuare al suo interno gli eventuali sottoinsiemi, tecnici e/o organizzativi, caratterizzati da omogeneità di requisiti ed obiettivi di sicurezza, all'interno dei quali potrà applicare in modo omogeneo le misure adatte** al raggiungimento degli obiettivi stessi

Inventario dei dispositivi autorizzati

- **ABSC 1: Inventario dei dispositivi autorizzati e non autorizzati**
- Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso
- Controlli principali:
  - Inventario delle risorse
  - Logging
  - Autenticazione di rete

Inventario dei software autorizzati e non

- **ABSC 2: Inventario dei software autorizzati e non autorizzati**
- Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione
- Controlli principali:
  - Inventario dei software autorizzati
  - Whitelist delle applicazioni autorizzate
  - Individuazione di software non autorizzato
  - Isolamento delle reti (air-gap)

Proteggere le configurazioni di HW e SW

- **ABSC 3: Proteggere le configurazioni di HW e SW sui dispositivi**
- Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.
- Controlli principali:
  - Configurazioni standard
  - Accesso amministrativo da connessioni protette
  - Verifica dell'integrità dei file critici
  - Gestione delle configurazioni

Correzione continua della vulnerabilità

- **ABSC 4: Valutazione e correzione continua della vulnerabilità**
- Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.
- Controlli principali:
  - Verifica delle vulnerabilità
  - Aggiornamento dei sistemi

Privilegi di amministratore

- **ABSC 5: Uso appropriato dei privilegi di amministratore**
- Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.
- Controlli principali:
  - Limitazione dei privilegi delle utenze amministrative
  - Inventario delle utenze amministrative
  - Gestione delle credenziali delle utenze amministrative

Difese contro i malware

- **ABSC 8: Difese contro i malware**
- Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni correttive.
- Controlli principali:
  - Sistemi di protezione (antivirus, firewall, IPS)
  - Uso dei dispositivi esterni
  - Controllo dei contenuti Web, email

Copie di sicurezza

- **ABSC 10: Copie di sicurezza**
- Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.
- Controlli principali:
  - Backup e verifica del restore
  - Protezione delle copie di backup

Protezione dei dati

- **ABSC 13: Protezione dei dati**
- Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti
- Controlli principali:
  - Uso della crittografia
  - Limitazioni sull'uso di dispositivi removibili
  - Controlli sulle connessioni di rete/Internet

Riferimenti

- Agenzia per l'Italia Digitale:
  - https://www.agid.gov.it
  - https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

- CERT-AgID:
  - https://cert-agid.gov.it
  - https://cert-agid.gov.it/pillole-informative/

Grazie per l’attenzione

corrado.giustozzi@acm.org