Sicurezza nelle grandi organizzazioni

Fabio Vernacotola

18/12/2018

Sezione 1

Progetti di sicurezza, perché…

Iniziative di sicurezza delle informazioni

Obiettivi strategici

- Direttamente correlati al core business dell'organizzazione
- Forniscono all'organizzazione un vantaggio competitivo

Esempi:

- Fornitore di servizi che offre servizi «sicuri» ai propri utenti (Marketing)
- Organizzazione che certifica ISO27001 i propri processi produttivi per poter accedere a gare pubbliche

Risk Management

…evitare gli incidenti ovvero l'impatto economico relativo alla perdita di:

- Riservatezza;
- Integrità
- Disponibilità

SAIPEM ENGINEERING ENERGY

SAIPEM ANNIVERSARY

Saipem: aggiornamento sull'attacco informatico subìto

San Donato Milanese (MI), 12 dicembre 2018 - In riferimento al comunicato del 10 dicembre 2018, Saipem comunica che l'attacco informatico ha colpito i server basati nel Middle East, India, Aberdeen e, in modo limitato, l'Italia attraverso una variante del malware Shamoon.

L'attacco ha comportato la cancellazione di dati e di infrastrutture, effetti tipici del malware.

Le attività di ripristino, in modalità graduale e controllata, sono in corso attraverso le infrastrutture di back-up e, quando completate, consentiranno la piena operatività dei siti impattati.

Saipem mantiene costanti contatti con le autorità competenti per ogni opportuna azione.

Saipem è uno dei leader mondiali nei servizi di perforazione, ingegneria, approvvigionamento, costruzione e installazione di condotte e grandi impianti nel settore oil&gas a mare e a terra, con un forte orientamento verso attività in ambienti difficili, aree remote e in acque profonde. Saipem fornisce una gamma completa di servizi con contratti su base "EPC" e/o "EPCI" ('chiavi in mano') e dispone di capacità distintive ed asset ad alto contenuto tecnologico.

CNN Money Markets Economy Companies Tech Autos India Video International

British Airways' latest tech problem is a major credit card hack

Yet another technical meltdown is plaguing British Airways. This time, hackers stole the payment card details of 380,000 customers.

The company said the data thieves made off with the names, addresses, emails and credit card details including the card number, expiration date and security code belonging to travelers who booked flights on British Airways' website and app between August 21 and September 5. No passport or travel details were taken.

Risk management

- Rischio = Probabilità di un evento avverso * impatto dell'evento avverso

L'obiettivo dell'organizzazione è quello di:

- limitare l'impatto;
- limitare la probabilità;

I rischi di sicurezza possono raggiungere valori economici molto significativi. Il costo medio di un mega data breach, ad esempio, è stato calcolato nel 2018 in 3,86 M$ *

* fonte Ponemon Institute 2018

Esempio: infezione ransomware su un server

- Impatto per:
  - Costo per indisponibilità delle applicazioni che utilizzano il server;
  - Costo di ripristino;
  - Costo di inoperatività del personale;

Mitigazione dell'impatto:

  - ridondanza dei server;
  - immagini virtuali ripristinabili in minor tempo possibile;

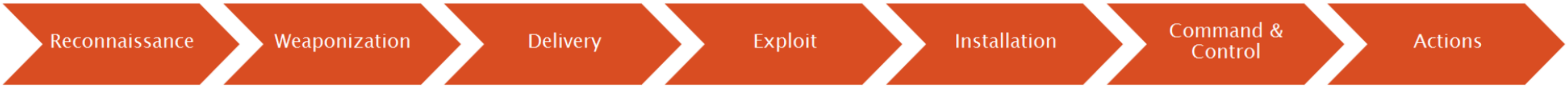
Esempio: infezione ransomware su un server

Ridurre la probabilità

Implementare contromisure come:

- Istruire i dipendenti (Security awareness);
- Limitare l'esecuzione di programmi sui server;
- Limitare l'uso di utenze privilegiate;

- In generale interrrompere la *kill chain* tipica degli attacchi ransom



Compliance – Conformità alla norme

E’ un obbiettivo dettato da obblighi di legge:

- Es. Conformità al Regolamento Europeo per la protezione dei dati personali 679/2016 (GDPR)
- Misure minime di sicurezza ICT per le pubblica amministrazioni emanate dall’AgID
- Direttiva NIS

O da accordi/contratti di servizio:

- PCI DSS (Payment Card Industry Data Security Standard)

GDPR – Regolamento UE 679/2016

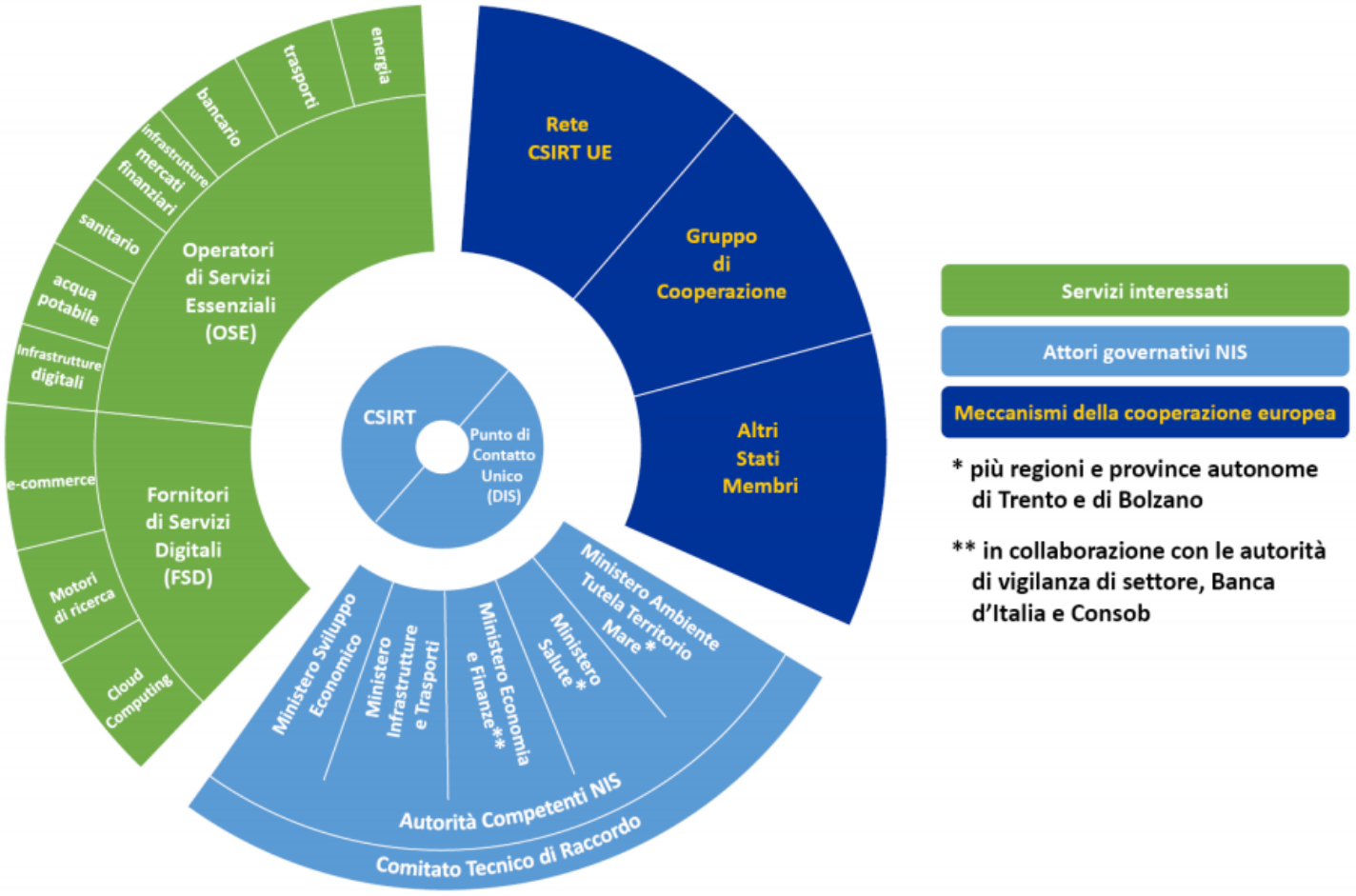
Art. 15 Right of access by the data subject	Art. 16 Right of rectification	Art. 17 Right to erasure (right to be forgotten)	Art. 18 Right to restriction of processing
Art. 20 Right to data portability	Art. 25 Data protection by design and by default	Art. 30 Records of processing activities	Art. 32 Security of processing
Art. 33 Notification of a personal data breach to the supervisory authority	Art. 35 Data protection impact assessment	Art. 47 Binding corporate rules	Art. 84 Penalties

Misure Minime Sicurezza ICT

- Pubblicate con circolare dell'Agenzia per l'Italia Digitale (AgID) n° 1/2017
- L'allegato 1 prescrive le misure minime di sicurezza informatica che "debbono essere adottate al fine di contrastare le minacce più comuni e frequenti" cui sono soggetti i sistemi informativi.
- Le amministrazioni devono realizzare gli adempimenti entro il 31 dicembre 2017
- La responsabilità dell'attuazione delle misure minime è posta in capo al responsabile dei sistemi informativi.
- Le modalità di attuazione delle misure minime devono essere descritte attraverso un modulo ad hoc che deve essere firmato digitalmente con marcatura temporale e presentate all'AgID su richiesta.

Direttiva NIS (1148/2016)

Network and Information Security



- Tanto gli **OSE** che gli **FSD**:
  - sono chiamati ad adottare **misure tecniche e organizzative adeguate e proporzionate** alla **gestione dei rischi** e a **prevenire** e **minimizzare l'impatto degli incidenti** a carico della sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio;
  - hanno l'**obbligo di notificare**, **senza ingiustificato ritardo**, gli **incidenti** che hanno un **impatto rilevante**, rispettivamente sulla continuità e sulla fornitura del servizio, al *Computer Security Incident Response Team* (CSIRT) italiano, informandone anche l'Autorità competente NIS di riferimento.

Come si valuta una iniziativa?

Conformità

Rischio

Strategia

?

Dimostrabilità del ritorno dell'investimento

Sezione 2

Stabilire quali iniziative intraprendere

Livello di maturità

- L’organizzazione è valutata rispetto a alcune dimensioni di analisi per determinare a livello macroscopico:
  - lo stato dell’organizzazione nei confronti della sicurezza;
  - il bilanciamento delle varie componenti.

- Importante per indentificare rapidamente:
  - l’entità di un programma di miglioramento della sicurezza;
  - gli ambiti su cui investire.

Security posture

- La security posture di una organizzazione è caratterizzata da:
  a. l'insieme delle misure di sicurezza scelte per la mitigazione dei rischi;
  b. grado di realizzazione delle misure di sicurezza scelte;

- Utilizzata principalmente per:
  - benchmarking;
  - gestione del rischio «framework based»;
  - stima della conformità;

Quale modello di maturità

SSE - Carnegie Mellon

PRISMA
IT Security ML

OWASP
OPENSAMM

Security Awareness MM

Resilience Management Model MIL

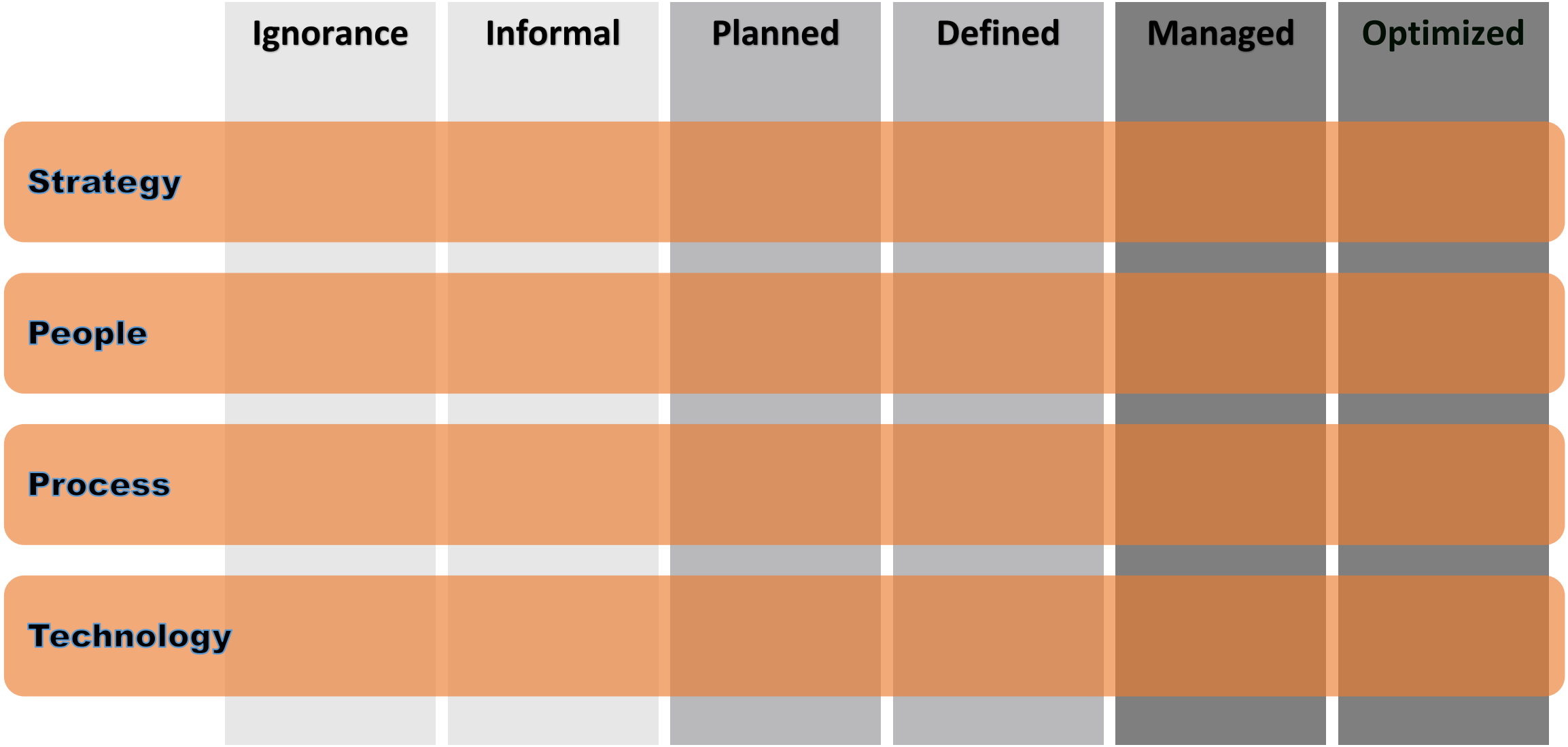
C2M2 - Department of Energy 1.1

Homeland Security NICE (Cybersecurity Initiative)

Information Security Forum MM

Framework for Improving Critical Infrastructure Cybersecurity

Esempio di Maturity Model (SEE-CMM)



Livelli di Maturità

Ignorance: non c'è evidenza di gestione della sicurezza
Informal: gestione della sicurezza attuata informalmente
Defined: presente il concetto di rischio. Acquisizione di elementi interni di valutazione.
Planned: gestione della sicurezza secondo processi definiti e coordinati
Managed (*Controlled*): gestione della sicurezza ben consolidata e oggetto di misurazione. Output quantitativamente predicibile.
Optimized: gestione della sicurezza proattiva e orientata al miglioramento continuo.

Framework di riferimento

- Insieme di «controlli», variamente organizzati, che definiscono cosa una organizzazione deve fare per poter gestire la propria sicurezza informatica.
- I framework rappresentano la formalizzazione di una «best practice» ma possono essere anche di derivazione normativa.
- Oltre a consentire una valutazione della security posture semplificano le attività di conduzione del proprio Sistema di Gestione della Sicurezza delle Informazioni, forniscono una base per le attività di audit interni.

SANS TOP 20

The **SANS Institute** is a private U.S. company that specializes in internet security training. It was founded in 1989 and provides computer security training, professional certification through Global Information Assurance Certification (GIAC), and a research archive - the SANS Reading Room.

1. Inventario dei device autorizzati e vietati;
2. Inventario dei software autorizzati e vietati;
3. Configurazione sicura per Hardware e Software su device mobili, portatili, workstation e server;
4. Vulnerability assessment continuo e relativa remediation;
5. Difesa dai Malware;
6. Sicurezza Applicativa;
7. Controllo dei device wireless;
8. Data recovery;
9. Security skill assessment a training appropriato;
10. Configurazione sicura dei device di rete;
11. Limitazione e controllo di porte, protocolli e servizi;
12. Uso controllato dei privilegi amministrativi;
13. Difesa "perimetrale";
14. Manutenzione, monitoraggio ed analisi dei log;
15. Controllo di accesso in ottemperanza al need to know;
16. Monitoraggio e controllo degli account;
17. Data Loss Prevention;
18. Incident Response and Management;
19. Ingegneria di rete sicura;
20. Penetration Test e addestramento;

Framework Misure Minime AgID

L'**Agenzia per l'Italia Digitale** è l'agenzia tecnica della Presidenza del Consiglio che ha il compito contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica.

CERT-PA: Computer Emergency Response Team Pubblica Amministrazione

AgID Basic Security Controls
ABSC 1 (CSC 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
ABSC 2 (CSC 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
ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER 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.
ABSC 4 (CSC 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.
ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.
ABSC 8 (CSC 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.
ABSC 10 (CSC 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.
ABSC 13 (CSC 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

Sezione 3

Lo standard ISO/IEC 27001:2013

Standard ISO/IEC 27001:2013

- E’ il più riconosciuto «standard» relativamente alla costituzione e gestione di un sistema di gestione della sicurezza delle informazioni (SGSI)
- Suggerisce come Stabilire, Attuare, Mantenere e Migliorare in modo continuo un SGSI
- Include un modello di miglioramento continuo
- E’ parte di un famiglia più ampia ISO/IEC 27000 che include:
  - Un vocabolario: ISO/IEC 27000;
  - Linee guida per l’implementazione ISO/IEC 27002:2013;
  - Tecniche di misurazione delle performance ISO/IEC 27004
  - Tecniche di risk management ISO/IEC 27005;

Cos’è un SGSI

Secondo la ISO27000:

Un SGSI consiste nelle policy, procedure, line guida e risorse ed attvità associate gestate collettivamente dall’organizzazione allo scopo di porteggere gli asset informativi.

Un SGSI è un approccio sistematico per stabilire, realizzare, condurre, monitorare, rivedere, mantenere e migliorare la sicurezza delle informazioni aziendali al fine di supportare gli obiettivi di business.

Struttura dello Standard 1/2

La prima parte dello standard stabilisce gli aspetti organizzativi del SGSI

- Contesto dell'organizzazione
- Leadership
- Pianificazione
- Supporto
- Valutazione delle prestazioni
- Miglioramento continuo

Struttura dello Standard 2/2

L’allegato A contiene il framework organizzato in

- Domini
- Obiettivi di controllo
- Controlli (133)

Domini

- Politiche per la sicurezza delle informazioni
- Organizzazione della sicurezza delle informazioni
- Sicurezza delle Risorse Umane
- Gestione degli asset
- Controllo degli accessi
- Crittografia
- Sicurezza fisica e ambientale
- Sicurezza delle attività operative
- Sicurezza delle comunicazioni
- Acquisizione sviluppo e manutenzione dei sistemi
- Relazioni con i fornitori
- Gestione degli incidenti relativi alla sicurezza delle informazioni
- Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa
- Conformità

Allegato A

Dominio

Obiettivo di controllo

Controlli

A.5 Politiche per la sicurezza delle informazioni		
A.5.1 Indirizzi della direzione per la sicurezza delle informazioni		
Obiettivo: Fornire gli indirizzi ed il supporto della direzione per la sicurezza delle informazioni in accordo con i requisiti di business, con le leggi e con i regolamenti pertinenti.		
A.5.1.1	Politiche per la sicurezza delle informazioni	*Controllo* Un insieme di politiche per la sicurezza delle informazioni deve essere definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti.
A.5.1.2	Riesame delle politiche per la sicurezza delle informazioni	*Controllo* Le politiche per la sicurezza delle informazioni devono essere riesaminate ad intervalli pianificati o nel caso in cui si siano verificati cambiamenti significativi, al fine di garantirne sempre l'idoneità, l'adeguatezza e l'efficacia.

A.13 Sicurezza delle comunicazioni		
A.13.1 Gestione della sicurezza della rete		
Obiettivo: Assicurare la protezione delle informazioni nelle reti e nelle strutture per l'elaborazione delle informazioni a loro supporto.		
A.13.1.1	Controlli di rete	*Controllo* Le reti devono essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni.
A.13.1.2	Sicurezza dei servizi di rete	*Controllo* I meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete devono essere identificati e inclusi negli accordi sui livelli di servizio relativi alla rete, indipendentemente dal fatto che tali servizi siano forniti dall'interno o siano affidati all'esterno.
A.13.1.3	Segregazione nelle reti	*Controllo* Nelle reti si devono segregare gruppi di servizi, di utenti e di sistemi informativi.

ISO/IEC 27001:2013 – Protezione dal malware

Dominio 12 - Sicurezza delle Attività Operative

Obiettivo di controllo 12.2: Protezione dal Malware

Controllo 12.2.1: Controlli contro il malware

A.12.2.1	Controlli contro il malware	*Controllo* Devono essere attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti.

- Individuazione
- Prevenzione
- Ripristino
- Consapevolezza

ISO/IEC 27002 – Protezione dal malware

Protection against malware should be based on malware detection and repair software, information security awareness and appropriate system access and change management controls. The following guidance should be considered:

a) establishing a formal policy prohibiting the use of unauthorized software (see 12.6.2 and 14.2.);

b) implementing controls that prevent or detect the use of unauthorized software (e.g. application whitelisting);

c) implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blacklisting);

d) establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken;

e) reducing vulnerabilities that could be exploited by malware, e.g. through technical vulnerability management (see 12.6);

f) conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated;

g) installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the scan carried out should include:

   1) scan any files received over networks or via any form of storage medium, for malware before use;

   2) scan electronic mail attachments and downloads for malware before use; this scan should be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the organization;

   3) scan web pages for malware;

h) defining procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks;

i) preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements (see 12.3);

j) implementing procedures to regularly collect information, such as subscribing to mailing lists or verifying web sites giving information about new malware;

k) implementing procedures to verify information relating to malware, and ensure that warning bulletins are accurate and informative; managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malware, are used to differentiate between hoaxes and real malware; all users should be made aware of the problem of hoaxes and what to do on receipt of them;

l) isolating environments where catastrophic impacts may result.

Lo standard ISO/IEC 27001:2013

- Lo standard ISO/IEC 27001:2013 è certificabile per una organizzazione.
- La certificazione è pubblica è viene registrata in appositi registri. In Italia il registro è gestito da Accredia
  - https://www.accredia.it/banche-dati/

- Il processo di certificazione è formalmente stabilito, nei tempi nelle modalità e nei costi.
- La certificazione è soggetta a revisione triennale.
- La ISO 27002 NON è certificabile

Grazie

Fabio.Vernacotola@Avanade.com

Fabio.Vernacotola@Avanade.com

Fabio Vernacotola

Avanade Security Practice Lead Italia

Rome Area, Italy

Add profile section

More...

Avanade

Coventry University

See contact info

See connections (286)