Verso le nuove linee guida per la sicurezza nella P.A.

Alessandro Sinibaldi
Cyber security expert CERT-PA

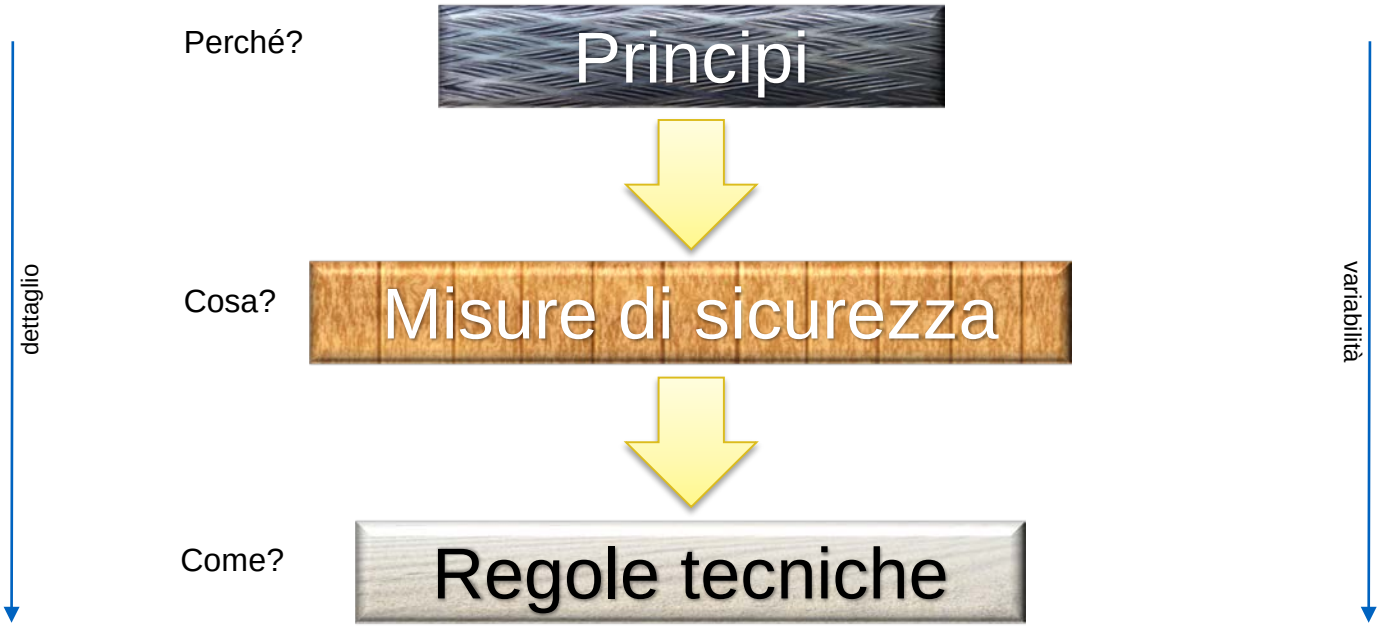
11/12/2018

Agenda

- I riferimenti
- Un modello a tre livelli
- 10 Principi di sicurezza
- Rapporto tra le linee guida e le misure minime

I riferimenti

- “Generally Accepted Information Security Principles (GAISP) Version 3.0.” del 2004 emanato da Information Systems Security Association (ISSA) (citadel-information.com/wp-content/uploads/2010/12/issa-generally-accepted-information-security-practices-v3-2004.pdf)
- Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione del 2002 (www.oecd.org/sti/ieconomy/15582268.pdf)
- ISO/IEC 27001
- «misure minime per le PP.AA.» emanate da AGID con la CIRCOLARE 18 aprile 2017, n. 2/2017 (https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict)


Perché?
Principi
Cosa?
Misure di sicurezza
Come?
Regole tecniche
dettaglio
variabilità

Devono essere garantite la **confidenzialità**, l'integrità e la disponibilità dei documenti trattati dalla PA

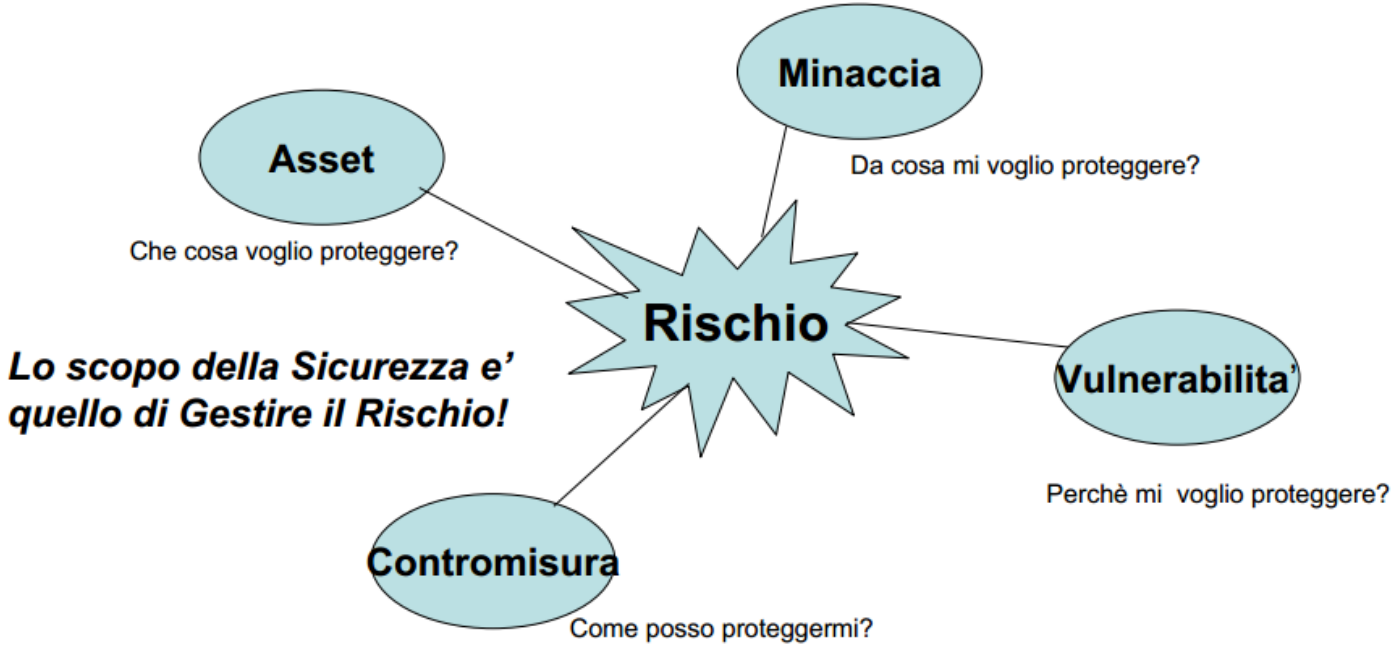
Tutti gli utenti devono essere autenticati con username e **password**

Le password devono essere lunghe almeno 8 caratteri e contenere numeri, lettere e caratteri speciali

Principio di inventario

questo principio si potrebbe riassumere nella massima “**conosci te stesso**”, intendendo con ciò che si deve sapere (e documentare) quali sono i propri **asset**, cioè quegli enti (persone, immobili, software, hardware, servizi, processi, competenze, dati, archivi ecc.) dove si trova il **Valore**, inteso non solo in senso economico, della propria organizzazione. Oltre a questo, è importante conoscere, dal punto di vista della sicurezza, quali sono le **minacce** a questi asset, quali le **vulnerabilità** e quali i **rischi** a cui si è sottoposti. Infine, conoscere gli asset vuol dire anche conoscerne le configurazioni

Principio di inventario



Lo scopo della Sicurezza e' quello di Gestire il Rischio!

Principio di attribuzione

Questo principio si riassume nella frase “**conosci chi fa cosa e cosa fa cosa, ha fatto o farà**”.

Dal punto di vista organizzativo, questo vuol dire attribuire **responsabilità chiare** ai ruoli coinvolti in un processo. Dal punto di vista tecnologico, bisogna gestire il **logging e il monitoring** degli eventi, in particolare quelli riferiti alla sicurezza. Dal punto di vista logico, vuol dire **gestire le autorizzazioni** in modo corretto ma anche gestire i **flussi di dati** (cosa va a chi) e gestire le operazioni sui dati (chi li crea, chi li legge, chi li modifica e chi li elimina).

Principio della pervasività

Questo principio può essere espresso con la frase “**La sicurezza deve essere come un abito**”.

Bisogna porsi nella situazione in cui la sicurezza è **pervasiva** nella propria organizzazione. Dal punto di vista applicativo, vuol dire sviluppare codice in modo sicuro secondo il paradigna **SD3** (Secure by Design, Secure by Default, Secure by Deploy). Dal punto di vista organizzativo, nei progetti è sempre presente una persona con competenze di sicurezza per analizzarne gli aspetti relativi.
Dal punto di vista logico, si usano metodologie, standard e best practices, si sviluppano policy e ci si accerta che vengano seguite, si fanno audit regolari e così via. L’obiettivo finale è che la sicurezza sia il più **trasparente** possibile agli utenti, cioè questi siano così ben formati (security awareness) che pensare e agire seguendo le best practice della sicurezza diventi automatico.

Principio della ridondanza

Questo principio esprime che “**tutto ciò che ha valore per un’organizzazione deve avere una copia o un possibile sostituto**”.

Dal punto di vista fisico, questo si traduce in infrastrutture di rete ridondate, RAID 5 per gli hard disk, utilizzo di backup regolari, server in load balancing o in cluster, locale o geografico, e più in generale **assenza di Single Point of Failure**.

Dal punto di vista organizzativo, invece, non ci devono essere uffici gestiti da una sola persona, competenze possedute solo da una persona e così via.

Dal punto di vista logico, occorre utilizzare, laddove possibile, l’autenticazione a più fattori invece che uno soltanto, inoltre, l’utente deve poter accedere a un servizio tramite più canali (es. sportello, web, mobile)

Principio del minimo

Una frase che riassume questo principio potrebbe essere “**Con il poco si gode, con il molto si tribola**”.

A prima vista, questo principio sembra antitetico rispetto al precedente ma si chiarisce subito pensando che mentre gli asset, cioè le cose importanti, devono essere ridondati, il contrario deve valere su tutto ciò che NON è importante.

Dal punto di vista della sicurezza ciò si traduce nella **minimizzazione della superficie di attacco** ad esempio installando sulle periferiche solo i servizi strettamente necessari. Dal punto di vista logico, bisogna fare **review periodiche** per accertarsi che tutto ciò che non serve più (come ad esempio vecchie utenze ancora presenti) sia eliminato, le autorizzazioni devono seguire i criteri del **minimo privilegio** e del **need to know**. Dal punto di vista organizzativo, si dovrebbero evitare procedure non necessarie, i processi dovrebbero essere semplificati, le catene di comando accorciate e così via.

Principio del miglioramento continuo

Questo principio si traduce nella constatazione che “**si può e si deve sempre fare di meglio**”

ed è anche un riflesso del fatto che il mondo evolve e non dobbiamo rischiare di rimanere indietro. Di fatto, è un invito a cavalcare il cambiamento, prevedendolo, facendolo proprio e non facendosi sorprendere. Dal punto di vista della sicurezza logica, questo ribadisce l’importanza di fare assessment con continuità, allo scopo di capire dove si è e dove si potrebbe andare. Inoltre, è importante che ci sia apprendimento continuo da parte dei dipendenti e, in particolare, di chi è coinvolto nella gestione della sicurezza. Bisogna tenersi sempre al corrente delle novità in campo tecnologico, normativo, di sicurezza ecc. La gestione dei rischi deve essere tenuta aggiornata sempre.

Principio dell’Automatizzazione

Questo principio può essere espresso in forme diverse. Da una parte, è un invito a cercare di ridurre il più possibile le attività manuali, limitandole soltanto alle fasi più creative dei progetti e dei processi. In questo caso, il vantaggio è un uso ottimale di risorse “pregiate” come il cervello umano ma anche una accresciuta trasparenza e velocità durante l’esecuzione e il fatto che il lavoro diventa sempre più prevedibile e sempre meno fatto in condizioni di emergenza. Alla base di una buona automatizzazione c’è la consapevolezza e la documentazione di ciò che si fa e di come lo si fa (e qui torniamo al Principio di Inventario). Dall’altra parte, dato che **non si può gestire ciò che non si può misurare**, un ulteriore aspetto importante è l’uso estensivo di misuratori obiettivi per conoscere lo stato di avanzamento dei processi e l’efficienza e l’efficacia con cui essi utilizzano le risorse e raggiungono i propri obiettivi.
Fare della buona automatizzazione, inoltre, comporta la gestione del **divario digitale** nell’uso delle tecnologie, la **formazione** degli utenti, l’uso delle best practice sull’**usabilità e accessibilità** delle interfacce uomo-macchina e l’utilizzo di standard architetturali nel disegno delle interfacce macchina-macchina.

Principio della temporalità

Questo principio invita a **lavorare per priorità** e a **garantire risposte tempestive** ai problemi di sicurezza (ad esempio installando le patch prima possibile) oltre che a impostare un sistema automatico di **allarmi** che intervenga tutte le volte che si verifichi una condizione di potenziale violazione di sicurezza. Inoltre, l'organizzazione deve essere in grado di **correlare eventi** che avvengono in momenti e in punti diversi della rete. Una delle conseguenze di questo principio è anche la capacità di **pianificazione** delle azioni e dei processi e dei progetti in generale e nella comprensione di quali attività possono essere svolte in serie, perché ognuna di esse sfrutta parte dell'output di quelle che la precedono, oppure in parallelo, portando così alla velocizzazione complessiva. Da un punto di vista pratico, gestire la tempistica vuol dire anche avere la percezione corretta di dove ci sono potenziali colli di bottiglia che rallentano e bloccano l'esecuzione dei processi portando a ritardi, a condizioni di errore e al lavoro in emergenza.

Principio della diversità

Anche in questo caso siamo in presenza di un principio che ha molteplici sfaccettature. Nella fase di elicitazione dei requisiti di sicurezza, occorre prendere in considerazione quelli espressi da tutti gli Stakeholder e, successivamente, risolvere eventuali conflitti tra di essi.
Inoltre, sia in fase di progettazione che facendo l'assessment di un sistema, è consigliabile cercare sempre di **assumere il punto di vista di un potenziale attaccante** e cercare di **pensare in modo "diverso" e creativo** e cioè come sia possibile bucare le proprie protezioni. Nella scelta di soluzioni di sicurezza può essere vincente utilizzare **prodotti di nicchia**, pur con le dovute attenzioni. Inoltre, se l'infrastruttura di sicurezza prevede più livelli, è consigliato utilizzare **soluzioni eterogenee** tra un livello e l'altro (ad esempio firewall di marca diversa) in modo che l'attaccante non possa sfruttare un'unica vulnerabilità e comunque raggiunga l'obiettivo con più difficoltà e lasciando più tracce. Questo principio ha anche una valenza culturale di rispetto e di promozione delle diversità: avere un team i cui partecipanti hanno pensieri, personalità e competenze diverse aiuta. Ricordiamoci che un approccio corretto alla sicurezza richiede **l'apertura alle critiche.**

Principio della separazione

Uno dei paradigmi chiave della sicurezza è quello della **Separation of duties**, che consiste nel far sì che, per completare un'attività, sia richiesta più di una persona, in modo da prevenire la possibilità di frode o errore. Tale ad esempio è, nella Costituzione italiana, la separazione dei poteri legislativo, esecutivo e giudiziario oppure il fatto che, per far partire un missile nucleare, due persone diverse devono far girare due chiavi separate in un cruscotto.
Inoltre, questo principio si manifesta nel creare ambiente fisici o virtuali che siano separati il più possibile gli uni dagli altri, in particolare se hanno esigenze di sicurezza diverse. Dal punto di vista logico, è consigliato **segmentare la rete** in Virtual LAN, separate da firewall, o anche creare **profili di autorizzazione diversi** per le varie operazioni di gestione oppure ancora, quando si deve trasmettere una password a un utente remoto, dividerla in due parti e trametterle su due canali separati. Dal punto di vista fisico, è consigliato **confinare gli apparati sensibili** in ambiti appositi, opportunamente protetti da accessi abusivi.

Principi e misure minime

ABSC 2.1.1 Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.

- Principio di Inventario
- Principio di Attribuzione
- Principio della Separazione
- Principio del Minimo

Principi e misure minime

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Principi
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.		I,A,S,M
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.		I,A,S
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).		I,A,S,M
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.		I,AU,A
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.		I,A,P
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.		I,P,A
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.		I,AU
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.		I,S

Il Paese che cambia passa da qui.

agid.gov.it cert-pa.it