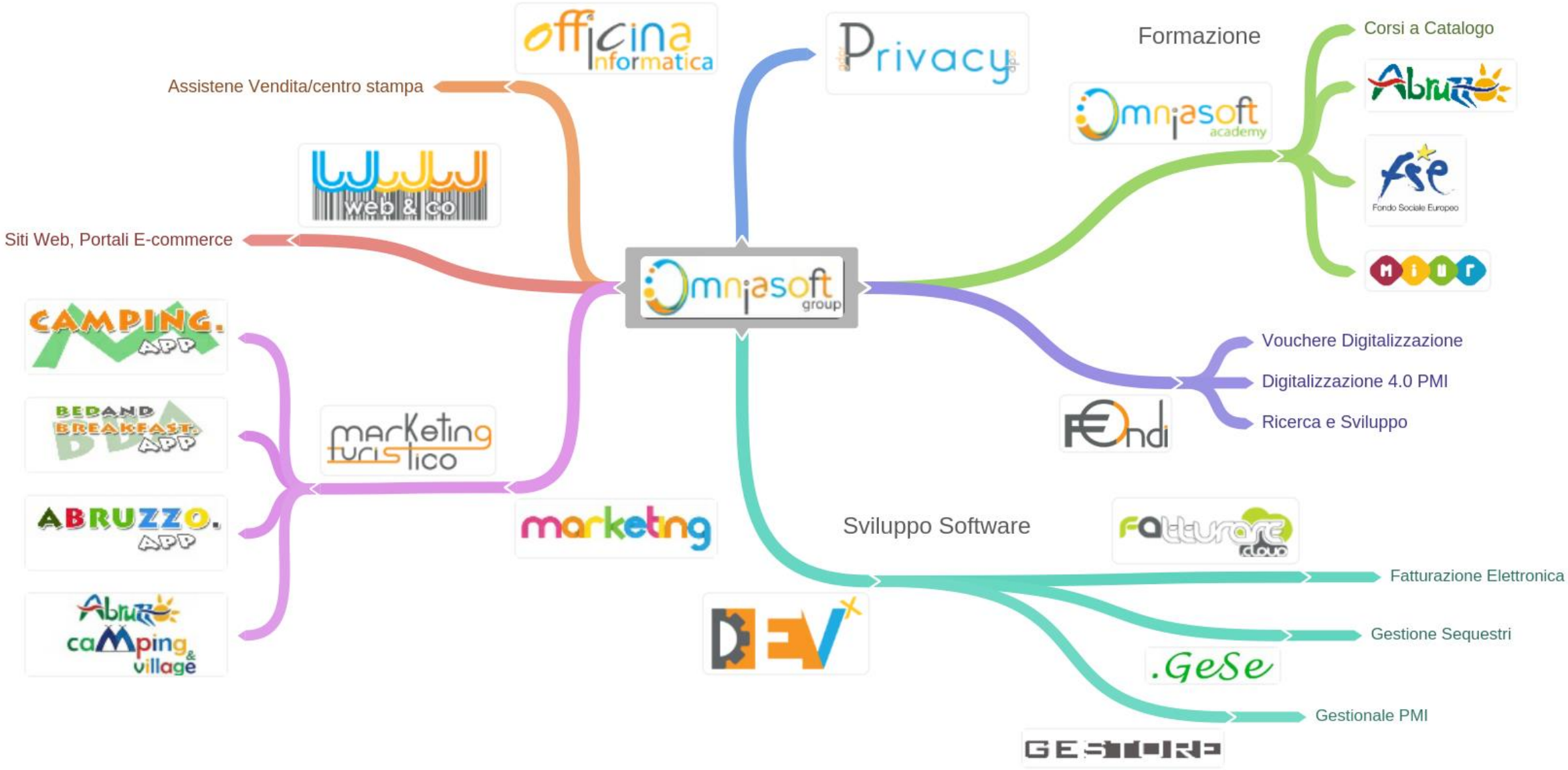
Privacy e Sicurezza Informatica nella scuola:
il nuovo regolamento europeo in materia di protezione dei dati personali

Francesco Guerrieri

▶ Ci presentiamo



Il processo di progettazione, come adeguarsi al GDPR 2016

Gli innovativi principi della privacy by design, privacy by default e accountability segnano un cambio di prospettiva per ogni titolare del trattamento che dovrà, prima ancora di iniziare il trattamento dei dati,

analizzare il contesto del trattamento, individuare i processi interni con i quali verranno trattati i dati e le risorse informatiche utilizzate.

Il processo di progettazione, quindi, avrà la finalità di:

- analizzare la natura dei dati personali, il contesto e le finalità del trattamento;
- individuare i soggetti che all'interno dell'organizzazione del titolare del trattamento sono autorizzati a trattare i dati personali;
- valutare le minacce ed il rischio per l'integrità e la perdita dei dati e conseguentemente individuare le misure di sicurezza tecniche ed organizzative adeguate.

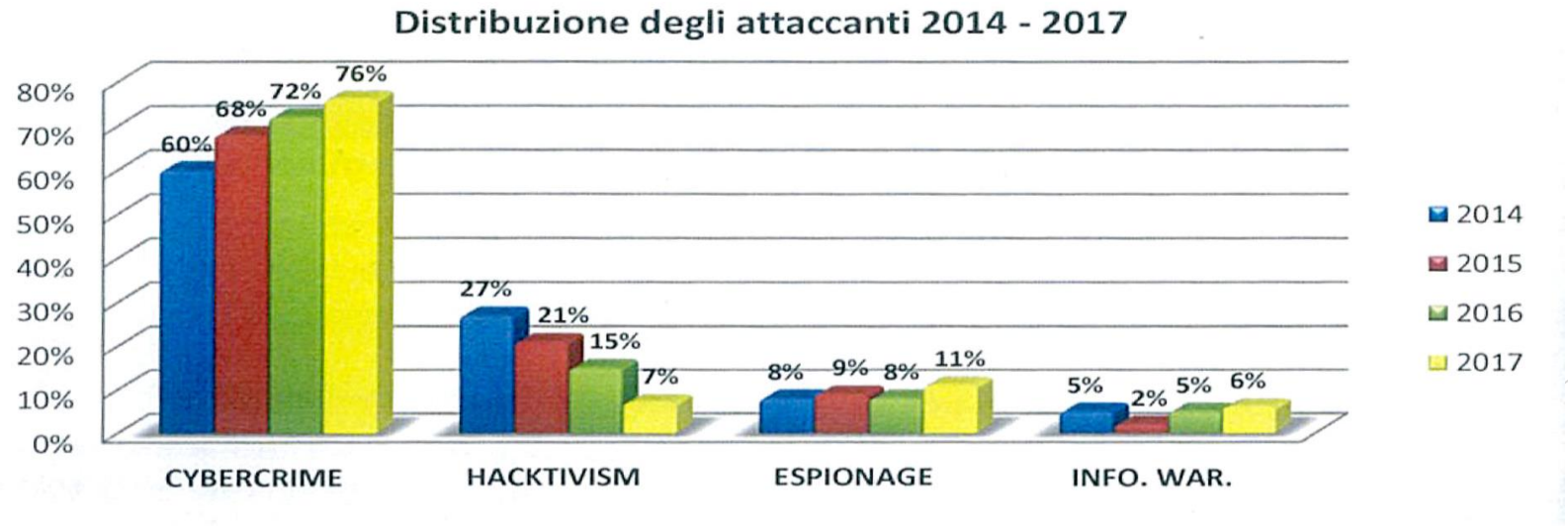
Le policy di sicurezza informatica nel nuovo Regolamento Europeo sulla privacy

- La sicurezza informatica è un elemento sempre più rilevante nell'ambito di aziende pubbliche e private, soprattutto in seguito alla maggior interconnessione dei sistemi ed il considerevole aumento dei servizi offerti attraverso la rete Internet.
- il proliferare e l'aumento del numero e della varietà dei dispositivi connessi alla rete, fa si che sia sempre più difficile avere una puntuale gestione della sicurezza informatica anche a causa di un elevato flusso di dati continuamente crescente e spesso ingestibile sotto il profilo della protezione delle risorse e delle informazioni aziendali.
- L'attuale generazione di cyber spionaggio – il cosiddetto hacker – rintraccia dati, informazioni e file cercando direttamente falle nei sistemi di sicurezza delle infrastrutture IT – ivi comprese le piattaforme Web (siti istituzionali, cloud, social network, ecc,) – mentre altri cyber-criminali si specializzano nella rivendita dei contatti e nei furti di identità.

- Vi è poi il noto fenomeno del “ramsonware” dove intere reti di computer e periferiche di memorizzazione vengono prese letteralmente in ostaggio con perdita di dati in caso del mancato pagamento di un riscatto.
- *Quindi, i titolari e i responsabili del trattamento nonché gli amministratori di sistema, sotto la cui responsabilità ricadono abitualmente le problematiche di sicurezza, si trovano anche in virtù dei dettati della normativa privacy alla protezione delle informazioni custodite all’interno dei sistemi e a verificare di conseguenza il corretto utilizzo degli apparati in uso agli utenti finali*.
- Si tratta di quelle *misure adeguate* definite nell’art. 32 del Regolamento U.E. 27 aprile 2016 n.679 anche se non meglio precisate sul piano tecnico.

Il panorama della sicurezza informatica in Italia e nel mondo

- A livello mondiale, **il cybercrime è risultato la prima causa di attacchi gravi ai sistemi informatici nel 2017** (76% del totale) per un danno complessivo stimabile in 500 miliardi di dollari (figura 1). In particolare, sono cresciuti, secondo l'ultimo Rapporto Clusit, gli attacchi d'information warfare (+24%) e di spionaggio con finalità politiche, industriali e di proprietà intellettuale (+46%) mentre è in calo l'hacktivism (-50%) ossia gli attacchi sostenuti da finalità ideologiche. Rispetto allo scorso anno, **si sono sperimentati più attacchi nei settori della ricerca/education (+29%), della vendita di software/hardware (+21%), del banking & Finance (+11%) e sanità (+10%)**. Meno bersagliati dello scorso anno i fornitori di servizi online e cloud (-47%), GDO/retail (-17%) e la pubblica amministrazione (-19%). **Nel 2017 sono cresciuti enormemente (+353%) gli attacchi classificati come "multiple targets" ossia rivolti a bersagli casuali, senza limiti territoriali, portati avanti con grandi mezzi e logiche industriali**. Clusit calcola che le sole attività truffaldine a danno dei privati cittadini – estorsioni, furti di denaro e di dati personali – abbiano colpito nel 2017 circa un miliardo di persone con un danno stimato in 180 miliardi di dollari.



- In questo panorama, pur se non espressamente previste, già da tempo le organizzazioni hanno adottato delle normative interne – comunemente denominate *policy* di sicurezza informatica o *security policy* – che indicano le misure organizzative e quali comportamenti debbano essere tenuti da dipendenti e collaboratori per contrastare i rischi informatici.
- E' ovvio, infatti, che l'atteggiamento imprudente nell'uso di internet, di workstation e di smartphone in ambienti lavorativi (come la scuola) può mettere a serio rischio tutta la struttura, con blocchi di produttività e, ora più che mai, di *data breach* ovverosia violazione di dati con tutti gli adempimenti che ne conseguono (art. 33 del medesimo sopraindicato Regolamento U.E.)

Non basta infatti studiare solo un piano di difesa informatica se poi un operatore disattende le procedure di sicurezza accettando *volontariamente* di eseguire un allegato di posta elettronica o aprire un improbabile file in quanto nessuno lo ha appositamente istruito!!!

Ma la sicurezza informatica scaturisce prima di tutto da una corretta percezione del personale (ata, docenti, etc.) e, in generale, da tutti coloro che utilizzano i servizi tecnologici messi a disposizione dalla scuola;

si parla quindi di una corretta formazione che deve essere preliminare all'uso dei dispositivi informatici stessi.

- ***Ogni policy va infatti esposta***, facendo comprendere agli interessati che sono parte attiva del processo di messa in sicurezza dei dati aziendali. Occorre spiegare il perché di ogni divieto e il perché sul PC o sullo smartphone aziendale non è possibile installare software e applicazioni non certificate (e men che meno di dubbia o illecita provenienza) ed anche perché è rischioso utilizzare piattaforme social e altre applicazioni online poco sicure con i laptop destinati all'uso aziendale.
- ***Chi definisce le policy*** interne deve anche farsi carico di formare e chiarire cosa sono ad esempio le attività di phishing (frode informatica finalizzata all'ottenimento di dati personali sensibili quali password, numero di carta di credito ecc. e perpetrata attraverso l'invio di un messaggio di posta elettronica a nome di istituti di credito, finanziarie, agenzie assicurative, in cui si invita l'utente, generalmente al fine di derubarlo, a comunicare tali informazioni riservate), cosa possono provocare e come evitarle. D'altra parte, l'azienda dovrebbe limitare le possibilità di "*errore*" magari filtrando anche le attività Web e i siti visitabili con azioni di *content filtering*(operazione di analisi e filtraggio di ogni parola chiave caricata nel *browser* indicata come "sconveniente" e quindi interdetta dai risultati dal motore di ricerca).
- ***La sensibilizzazione*** deve ottenere un effetto formativo: ad esempio dovrebbe essere compreso da tutti che un qualsiasi dispositivo informatico che appartenga o che transiti in azienda dovrebbe essere validamente protetto e che, su tutti i PC e, comunque qualunque dispositivo che si colleghi alla rete aziendale, dovrebbe aver installato un antivirus e un software anti-malware professionale aggiornati quotidianamente.

Molta attenzione, ad esempio, dovrebbe essere riposta nelle cautele volte a:

- mantenere segrete le proprie credenziali di accesso (password e/o pin);
- non lasciare libero accesso ai propri dispositivi in caso di assenza momentanea dalla propria postazione lavorativa;
- controllare l'accesso ad internet ed ai servizi di posta elettronica;
- verificare la presenza di eventuali tracce malevoli prima di utilizzare supporti rimovibili, quali pendrive e memory card;
- curare l'osservanza di backup periodici;
- evitare per l'uso di dispositivi scolastici al di fuori dell'ambito lavorativo.
- ecc.

Tuttavia, le policy devono anche riflettere le realtà dell'istituto e vanno quindi create e modulate sulla reale contingenze della scuola evitando anche il segno opposto cioè quello di ingessare la stessa con pratiche o procedure inutili ed ininfluenti sul piano della sicurezza informatica.

Considerazioni

Nel panorama italiano non esistono indicazioni formali da seguire nella compilazione delle policy di sicurezza informatica per cui il tutto viene lasciato all'inventiva ed alla capacità di titolari e responsabili che debbono prima esaminare il contesto organizzativo interno e poi produrre adeguate norme di comportamento, tenendo anche conto dell'evoluzione tecnologica dei sistemi e quindi della necessità di dover adeguare nel tempo le stesse policy.

E' importante nella creazione delle stesse regole effettuare una preliminare analisi del rischio in modo da bilanciare la formulazione delle stesse direttive.

Un modello corretto di formulazione delle policy connesso ad una piena comprensione delle stesse regole potrebbe consentire un ulteriore innalzamento delle difese da attacchi cibernetici e permettere all'aziende di operare con maggiore serenità.

BIBLIOGRAFIA
REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Cosa fare?

Affidarsi al parere degli esperti può pertanto essere utile per capire con chiarezza da dove iniziare.

Di seguito i (primi) **sei passi** fondamentali da compiere, soprattutto alla luce delle nuove direttive.

- **Sapere quali sono i dati da proteggere (e dove sono)**. Capire di quali dati dispone la propria organizzazione, dove si trovano e chi ne è responsabile è fondamentale per la costruzione di una buona strategia di data protection.
- **Formare i dipendenti**. La privacy e la sicurezza dei dati sono una parte fondamentale del nuovo GDPR, quindi è fondamentale che il personale sia pienamente consapevole dell'importanza di questo processo. Statisticamente, infatti, gli esperti rilevano che i problemi di sicurezza IT più comuni e rovinosi sono proprio dovuti a errori umani. Ad esempio, la perdita o il furto di una chiavetta USB o di un portatile contenente informazioni sensibili relative all'attività aziendale potrebbe seriamente danneggiare la reputazione dell'organizzazione, o addirittura portare a severe sanzioni pecuniarie.
- **Creare un elenco dei dipendenti che hanno accesso ai dati sensibili**. Proprio perché l'errore umano è foriero di molti problemi relativi alla sicurezza dei dati, mantenere un controllo serrato su chi, tra i dipendenti, può accedere a quali informazioni è estremamente importante. Occorre ridurre al minimo i privilegi e concedere l'accesso solo ai dati di cui ogni risorsa ha effettivamente bisogno. Inoltre, l'inserimento di *watermark* (il marchio digitale che identifica l'autore di un file video, audio o di un'immagine, mediante un'invisibile trama di bit contenente le informazioni sul copyright, ndr) nei file può aiutare a prevenire il furto di dati da parte del personale e permette di identificare la fonte in caso di violazione. Questa pratica prevede l'aggiunta al database di record di rilevamento unici (i cosiddetti seed) che offrono la possibilità di monitorare il modo in cui i dati vengono utilizzati e *tracciare* il loro percorso, anche nel caso in cui vengano spostati al di fuori del controllo diretto dell'organizzazione.

- **Effettuare un’analisi dei rischi**. Gli esperti consigliano di effettuare regolari valutazioni del rischio per individuare eventuali potenziali pericoli per i dati dell’organizzazione. Con questa prassi dovrebbero essere esaminati tutti i tipi di minaccia identificabili (sia digitali che fisici): dalla violazione dei dati online, alle interruzioni di corrente. In questo modo è possibile identificare eventuali punti deboli nel sistema di sicurezza aziendale, stabilire le priorità e formulare quindi un preciso piano d’azione per evitare danni, riducendo così il rischio di dover poi far fronte a una violazione ben più costosa.
- **Installare il software di protezione affidabili ed eseguire scansioni regolari**. Una delle misure più importanti per la protezione dei dati è anche una delle più semplici. Con un buon sistema di prevenzione attiva e scansioni regolari è infatti possibile ridurre al minimo la minaccia di una perdita di dati per mano di criminali informatici. Investire in un buon software antivirus e antimalware – sempre all’interno di una più completa strategia di sicurezza informatica – aiuterà a non far cadere le informazioni sensibili nelle mani sbagliate.
- **Eseguire regolarmente il backup dei dati più importanti e sensibili**. Effettuare un backup regolare è una pratica spesso trascurata, ma secondo gli esperti poter contare su una continuità di accesso alle informazioni rappresenta una dimensione fondamentale della sicurezza IT. Se si considera quanto tempo e quali sforzi potrebbero essere necessari per recuperare i dati perduti, appare subito chiaro come gestire una strategia di backup sia una mossa vincente.

Alcune soluzioni

1. Installazione e configurazione di sistemi Firewall
2. Creazione di sistemi software/hardware di backup automatico
3. Acquisto di soluzioni di backup anche in cloud
4. Creazione di regole informatiche ben precise ad-hoc per ogni struttura
5. Creazione di procedure cartacee per la consegna di credenziali
6. Configurazione livello sicurezza pc/dispositivo medio/alto
   - Gestione degli utenti
   - Gestione dei ruoli
   - File di log per eventuali controlli

REGOLAMENTO PRIVACY NELLE SCUOLE

Se volessimo seguire tutto quello che il nuovo GDPR ci ‘consiglia’…
cosa dovremmo fare?

Cosa devono fare gli istituti scolastici o strutture ben organizzate?

Ecco cosa fare nello specifico:

- INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI
- INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
- PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
- VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
- USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
- DIFESE CONTRO I MALWARE
- COPIE DI SICUREZZA
- PROTEZIONE DEI DATI

INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

- Implementare un inventario delle risorse attive
- Implementare un inventario attraverso uno strumento automatico
- Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie
- Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico
- Implementare il "logging" delle operazione del server DHCP
- Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite
- Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete
- Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete
- Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP
- Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.
- Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.
- Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.
- Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.

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.

- 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'istallazione di software non compreso nell'elenco.
- 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.
- 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).
- Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.
- Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.
- Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.
- 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.
- 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.

PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

- Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.
- Le configurazioni sicure standard devono corrispondere alle versioni “hardened” del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.
- Assicurare con regolarità la validazione e l’aggiornamento delle immagini d’installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.
- Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall’organizzazione.
- Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.
- "Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestionedei cambiamenti."
- Le immagini d’installazione devono essere memorizzate offline.

- Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.
- Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).
- Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.
- Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.
- Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.
- I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.
- Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.
- Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.

VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

- Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche
- Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.
- Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).
- Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.
- Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un Account dedicato che non deve essere usato per nessun'altra attività di amministrazione.
- Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.
- Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
- Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità.
- Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.

- Assicurare l’aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.
- Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.
- Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.
- Rivedere periodicamente l’accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.
- Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).
- "Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischioassociato, partendo dalle più critiche."
- Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall’organizzazione.
- Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.

VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

- Eseguire periodicamente la ricerca delle vulnerabilità con frequenza commisurata alla complessità dell'infrastruttura.
- Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).
- Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.
- Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un Account dedicato che non deve essere usato per nessun'altra attività di amministrazione.
- Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.
- Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
- Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità.
- Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.

- Assicurare l’aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.
- Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.
- Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.
- Rivedere periodicamente l’accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.
- Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).
- "Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato, partendo dalle più critiche."
- Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall’organizzazione.
- Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.

USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

- Limitare i privilegi se non si hanno le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi
- Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.
- Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.
- Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.
- Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.
- Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga
- Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.
- Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.

- Generare un’allerta quando viene aggiunta un’utenza amministrativa.
- Generare un’allerta quando vengano aumentati i diritti di un’utenza amministrativa.
- Tracciare nei log i tentativi falliti di accesso con un’utenza amministrativa.
- Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L’autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.
- Quando l’autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).
- Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.
- Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).

- Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).
- Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.
- Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.
- Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.
- Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.
- Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.
- Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.
- Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.
- Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).
- Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.
- Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.

DIFESE CONTRO I MALWARE

- Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.
- Installare su tutti i dispositivi firewall ed IPS personali.
- Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.
- Tutti gli strumenti censiti sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.
- È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi antimalware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.
- L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.
- Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.

- Monitorare l’uso e i tentativi di utilizzo di dispositivi esterni.
- Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.
- Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.
- Usare strumenti di filtraggio che operano sull’intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.
- Installare sistemi di analisi avanzata del software sospetto
- Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.
- Disattivare l’esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.

- Disattivare l’esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.
- Disattivare l’apertura automatica dei messaggi di posta elettronica.
- Disattivare l’anteprima automatica dei contenuti dei file.
- Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.
- Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l’impiego di strumenti antispam.
- Filtrare il contenuto del traffico web.
- Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l’organizzazione ed è potenzialmente pericolosa (e.g. .cab).
- Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento
- Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.

COPIE DI SICUREZZA

- Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.
- "Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backupdevono riguardare il sistema operativo, le applicazioni software e la parte dati."
- Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.
- Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.
- Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud
- Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.

PROTEZIONE DEI DATI

- Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica
- Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti
- Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.
- Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.
- Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/ configurazioni che impediscano la scrittura di dati su tali supporti.

- Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi
- Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.
- Individuare anomalia rispetto al normale traffico di rete, che deve essere registrata anche per consentirne l'analisi off line.
- Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.
- Bloccare il traffico da e verso url presenti in una blacklist.
- Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository

Esempi pratici

Negli anni abbiamo avuto modo di studiare e risolvere molti casi che ad oggi sono per noi esempio pratico da ‘curare’ per la messa a norma della privacy ma soprattutto per la difesa personale contro attacchi non desiderati.

- ✓ Furto di identità (attraverso i social)
- ✓ Maleware ‘fastidiosi’ che usano il vostro dispositivo per altri servizi
- ✓ invio di mail a propria insaputa con dati sensibili (sia dell’utente colpito sia di utenti collegati)
- ✓ Acquisto di merce su siti e-commerce non protetti (http e non https)
- ✓ Accesso a tutti i contenuti personali presenti sul proprio dispositivo
- ✓ Registrazione sia audio che video da remoto senza il consenso del proprietario del dispositivo

in the age of information ignorance is a choice.

Francesco Guerrieri
Data Analysis Manager
I.C.T.& I.O.T. Specialist
Direttore Agenzia Formativa
Chief privacy officer

info@omniasoft.it

.aule e laboratori: via Senarica 11
.office &store: via Latini (angolo via Garibaldi)
Roseto Degli Abruzzi (Te) _tel_ 085_8941866