Allegato 1 - Privacy policy

L'impatto del GDPR in ambito scolastico

Il trattamento dei dati personali in ambito scolastico implica una serie di problematiche su più livelli: da quelle relative alla struttura tecnologica e alle modalità operative interne, a quelle legate sicurezza e alla consapevolezza nell'utilizzo degli strumenti a disposizione delle organizzazioni.

Un approfondito esame della disciplina europea e nazionale e la concreta applicazione della stessa, ha evidenziato che quanto richiesto non è un'incombenza meramente formale, ma un punto di approdo, sì difficile da raggiungere, ma non irraggiungibile.

Riservatezza, integrità e disponibilità dei dati

Il Regolamento Europeo, così come la disciplina interna, sono diretti a individuare i presupposti per considerare legittimi i trattamenti dei dati personali compiuti dalle organizzazioni. Conseguentemente non può essere fatta una valutazione soltanto per ciò che concerne la **riservatezza** dei dati, in quanto le norme prevedono la necessità di approfondire anche gli aspetti dell'**integrità** e della **disponibilità** degli stessi.

Per raggiungere questo ambizioso obiettivo, nel rispetto del principio **dell'accountabilty**, è importante attuare un percorso diretto all'incremento dei livelli di sicurezza e di consapevolezza nell'utilizzo degli strumenti a disposizione delle organizzazioni.

La sicurezza degli strumenti digitali

Tutte le attività vengono svolte attraverso sistemi informatici che mediante il loro utilizzo elaborano e conservano i dati personali delle svariate categorie interessate (studenti, famiglie, personale dipendente, fornitori).

Tali dati vengono conservati nei server o nei cloud della scuola o delle applicazioni in uso alla scuola mentre i fascicoli cartacei esistono soprattutto come duplicazioni delle stesse informazioni, in versione analogica.

Le workstation utilizzate per le attività amministrative sono dotate di sistemi di sicurezza: sistemi operativi autentici e sempre aggiornati, antivirus e firewall, procedura di autenticazione personale mediante password con caratteristiche adeguate, disaster recovery.

GDPR e sicurezza digitale

Il tema della sicurezza informatica riveste un'importanza fondamentale e strategica. Ciò è ancor più evidente se si considera il costante aumento delle violazioni (più o meno rilevanti) ai sistemi informatici o le numerose perdite di dati e di informazioni dovute a comportamenti negligenti o imprudenti dei dipendenti pubblici o, ancora, a malfunzionamenti dei sistemi informatici o telematici.

La sicurezza informatica, infatti, ha lo scopo di minimizzare i rischi che incombono sulle informazioni digitali (non solo sui dati personali in essi contenuti) andando a perseguire il raggiungimento di tre obiettivi: la confidenzialità (o, come l'abbiamo definita in precedenza, riservatezza), l'integrità e la disponibilità delle informazioni.

Il data breach secondo il GDPR

A seguito di una violazione di dati personali (data breach) è prevista una procedura specifica e molto delicata.

A livello normativo, il GDPR introduce all'art. 4, par. 12, la definizione di violazione dei dati: "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

La disciplina del data breach, pur essendo inquadrabile nell'ambito del risk management, riguarda chiaramente la gestione ex post degli eventi pregiudizievoli.

In generale si è in presenza di un data breach ogni qualvolta ci sia una violazione di dati personali che incida su uno dei tre aspetti relativi alla sicurezza, ovvero riservatezza, integrità e disponibilità dei dati personali.

Un data breach esiste in quanto tale, indipendentemente dalla sua imputabilità o dalle sue cause. Pertanto è irrilevante, ai fini dell'obbligo di notifica o di comunicazione, che l'evento sia imputabile ad azioni di terzi (per es. attacco informatico) o che sia invece meramente accidentale.

In caso si valuti di dover procedere alla notifica, questa dovrà essere fatta senza ingiustificato ritardo, ovvero entro settantadue ore dal momento in cui si ha avuto conoscenza dell'avvenuta violazione. In caso di ritardo nella notifica, occorrerà specificare i motivi del ritardo. A livello contenutistico la notifica dovrà prevedere: la descrizione della natura della violazione e, se possibile, le categorie e il numero approssimativo di interessati coinvolti; la comunicazione del nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; la descrizione delle probabili conseguenze della violazione; la descrizione delle misure adottate, o in fase di adozione, per rimediare alla violazione e, laddove possibile, per attenuarne i possibili effetti negativi.

In caso tutte queste informazioni non si possano fornire contestualmente, si potranno anche fornire in fasi successive, adducendo i motivi del ritardo. Ciò permette di poter assolvere all'obbligo di notifica nelle settantadue ore, specificando meglio le modalità di intervento in un successivo momento.

All'obbligo di notifica l'art. 34 del GDPR aggiunge l'obbligo della comunicazione del data breach anche all'interessato. Ciò è previsto solamente nei casi in cui la violazione rappresenti un rischio elevato per i diritti e le libertà delle persone fisiche. In tali casi la comunicazione è da effettuarsi "senza ingiustificato ritardo", e deve descrivere la natura della violazione con un linguaggio chiaro e preciso. Anche in questo caso la comunicazione ha un contenuto minimo, costituito, oltre che dalla descrizione della natura della violazione, anche dal nome e dai dati di contatto del responsabile della protezione dei dati (o di altro punto di contatto presso cui ottenere più informazioni); dalla descrizione delle probabili conseguenze della violazione; dalla descrizione delle misure adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Il GDPR e le misure di sicurezza informatica a protezione della Privacy

La sicurezza nell'informatica equivale ad attuare tutte le misure e tutte le tecniche necessarie per proteggere l'hardware, il software ed i dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza, nonché eventuali usi illeciti, dalla divulgazione, modifica e distruzione.

Per il legislatore comunitario la sicurezza delle reti e dell'informazione si sostanzia nella capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica, gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza.

Ciò ovviamente comprende anche misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica.

Per mantenere la sicurezza e prevenire trattamenti in violazione al GDPR, il titolare del trattamento deve valutare anche il rischio informatico che può essere definito come il rischio di danni economici (rischi diretti) e di reputazione (rischi indiretti) derivanti dall'uso della tecnologia, intendendosi con ciò sia i rischi impliciti nella tecnologia (i cosiddetti rischi di natura endogena) che i rischi derivanti dall'automazione, attraverso l'uso della tecnologia, di processi operativi aziendali (i cosiddetti rischi di natura esogena).

In particolare questi ultimi possono essere:

- danneggiamento di hardware e software;
- errori nell'esecuzione delle operazioni nei sistemi;
- malfunzionamento dei sistemi;
- programmi indesiderati.

Principio di sicurezza

L'art. 5, par. 1, lett. f), stabilisce che i dati personali devono essere "trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)". È importante notare che è l'intero trattamento a dover essere sicuro, non solo i dati come prodotto finale. Ciò comporta anche che le valutazioni di sicurezza vanno sviluppate per ogni tipo di trattamento.

L'art. 32, invece, fissa alcuni principi fondamentali. In particolare le misure di sicurezza devono essere approntate "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche".

Le misure di sicurezza, quindi, devono essere adeguate, imponendo non un'obbligazione di risultato, bensì un'obbligazione di mezzi, in modo che le misure siano ragionevolmente soddisfacenti alla luce delle conoscenze e delle prassi.

Le misure di sicurezza si dividono in due categorie: misure organizzative e misure tecniche, che, sempre secondo l'art. 32, comprendono, tra le altre:

a) la pseudonimizzazione e la cifratura dei dati personali (misura tecnica);
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (requisiti di sicurezza);
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

La sicurezza, infatti, non riguarda solo l'aspetto informatico del trattamento, ma anche l'aspetto organizzativo a coprire eventi quali la sottrazione o la perdita di documenti. Le misure di sicurezza, quindi devono garantire che:

- i dati possono essere consultati, modificati, divulgati o cancellati solo dalle persone autorizzate a farlo (e che tali persone agiscono solo nell'ambito dell'autorità che gli viene concessa);
- i dati trattati sono accurati e completi in relazione al motivo per cui lo stai elaborando;
- i dati rimangono accessibili e utilizzabili, cioè, in caso di perdita, modifica o distruzione accidentale, si deve essere in grado di recuperarli e prevenire danni alle persone interessate, predisponendo un opportuno piano di continuità operativa.

Misure di sicurezza fisiche
Per approntare delle misure di sicurezza è necessario valutare fattori quali:

- la qualità delle porte e delle serrature e la protezione dei locali con allarmi, illuminazione di sicurezza o CCTV (telecamere);
- l'accesso ai locali e il controllo dei visitatori;
- il corretto smaltimento dei rifiuti cartacei o elettronici;
- la sicurezza delle apparecchiature informatiche, in particolare i dispositivi mobili (è utile tenere un registro con l'indicazione delle risorse informatiche utilizzate per trattare dati, la loro ubicazione fisica e i permessi di accesso alle stesse).

Misure di sicurezza informatiche (o logiche)
Fattori da considerare per la sicurezza informatica:

- sicurezza della rete e dei sistemi di informazione (sistemi di autenticazione);
- sicurezza dei dati conservati nel sistema (controlli di accesso);
- sicurezza online (sito web o applicazioni online);
- sicurezza dei dispositivi, in particolare quelli personali se usati per motivi aziendali.

I sistemi di autenticazione devono essere configurati in modo da controllare gli accessi ai dispositivi e agli applicativi, tramite credenziali (username e password). La politica in materia di password dovrebbe essere definita a documentata, con indicazione della lunghezza minima e dei criteri per la scelta delle password. Ancora meglio sarebbe utilizzare sistemi di verifica a due fattori (2FA). Laddove possibile sono da preferire profili con privilegi distinti e compiti separati.

Rischio del trattamento

Il Considerando 75 ci aiuta con riferimento al concetto di rischio: "I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati".

Si tratta di uno dei criteri previsti dal regolamento generale per la progettazione dei trattamenti, che appunto prevede l'obbligo di una analisi del rischio del trattamento, e quindi della valutazione delle misure tecniche od organizzative che il titolare ritiene di dover adottare per ridurre l'eventuale rischio.

Per ogni rischio occorre individuare la probabilità dell'evento, nonché la gravità dello stesso. Un esempio classico riguarda la dismissione delle stampanti con memoria, senza aver provveduto a cancellare la memoria, e quindi con l'astratta possibilità che un terzo possa acquisire le immagini ottiche degli ultimi documenti stampati o scansionati.

Tipi di rischio

- **Trattamento (raccolta) di dati non necessario in base alla finalità**
  Vedi art. 5, par. 1 lett. b) (principio di finalità), art. 13
- **Informativa e termini non chiari o trasparenti**
  Vedi art. 4, par. 11 (consenso dell'interessato) e art. 13
- **Dati personali non aggiornati o obsoleti**
  Vedi art. 15 e 16 (diritto di rettifica) Perdita di dati lato operatore
  Vedi art. 32 (misure di sicurezza)
- **Inefficace o intempestiva cancellazione dei dati personali**
  Vedi art. 17 (diritto alla cancellazione)
- **Condivisione di dati con terze parti**
  Vedi art. 7 (condizioni per il consenso), inoltre anche art. 21 (diritto di opposizione) e 22 (processi decisionali automatizzati)
- **Trasferimento dati non sicuro**
  Vedi art. 32 (misure di sicurezza)
- **Comunicazione non tempestiva delle violazioni di dati**
  Vedi art. 33 e 34 (notifica violazione dati e comunicazione all'interessato)
- **Vulnerabilità delle applicazioni web**
  Vedi art. 32 (misure di sicurezza)

La Check-List della Sicurezza IT

Preoccuparsi della sicurezza dei dati e della privacy nella navigazione Internet, è anche avere piena consapevolezza di quanto sia importante proteggere il computer e tenerlo lontano da intrusioni esterne.

L'argomento sicurezza Internet si può dividere in quattro parti:

1. protezione del computer e della rete;
2. sicurezza delle password;
3. sicurezza del browser;
4. navigazione su reti wifi.

Sicurezza del computer

- É stato installato un antivirus?
- L'antivirus si aggiorna automaticamente ogni giorno?
- Se non è stato ancora installato un antivirus oppure se la protezione è scaduta e non si aggiorna più, bisogna provvedere quanto prima al rinnovo della protezione o passare a un antivirus gratuito. L'antivirus è la prima protezione del nostro pc.
- É attivo il firewall di Windows?
- Sono attivi gli aggiornamenti automatici del sistema operativo?
  Molti trascurano questo aspetto e lo vedono più come un fastidio. Invece tali aggiornamenti sono patch di sicurezza che vanno a coprire gli ultimi buchi scoperti che permettono a utenti malintenzionati di entrare nei pc dall'esterno e prenderne il controllo. Questo discorso vale anche per sistemi operativo non Windows perché è da dimenticare il luogo comune che i sistemi non Windows sono immuni da virus e quant'altro.
- Abbiamo impostato un piano di backup dei dati, dei documenti e delle foto?
  Per la sicurezza di non perdere i file creati e salvati sul computer, pianificare il backup automatico così da poterne avere una doppia copia di sicurezza.
- Teniamo aggiornati i programmi installati sul computer?
  Come per il sistema operativo, anche per i programmi escono spesso aggiornamenti di sicurezza.
- Quando scarichiamo programmi, è indispensabile fare attenzione, nella procedura di installazione a non installare anche altri software "consigliati"?
  Purtroppo, molti programmi gratis sono accompagnati da sponsor, cosiddetti "crapware", sotto forma di programmi non richiesti che si installano automaticamente.
  Nel caso, fare un controllo per trovare e rimuovere programmi e toolbar inutili che rallentano il computer.

Sicurezza del browser

Il fatto che il computer sia protetto da virus e da intrusioni esterne non garantisce che la navigazione sia comunque sicura e privata. Molte persone possono non preoccuparsi della privacy, ma la sicurezza resta comunque fondamentale.

- Quando facciamo il login con password ad un sito, è bene controllare sempre che l'indirizzo inizi con https.
  HTTPS è il protocollo della connessione cifrata e si differenzia rispetto al normale http per il fatto che ogni dato trasmesso è crittografato. Questo significa che, anche volendo sniffare il traffico di rete, è illeggibile per chiunque, compresi i gestori di quel sito.
- Sappiamo riconoscere, a occhio, i siti pericolosi in cui bisogna stare attenti a dove si clicca?
- Quando ci colleghiamo ad un sito da un computer non usato solo da noi, facciamo sempre la disconnessione?

Ricordare sempre e comunque di fare il logout di tutti gli account, soprattutto su computer pubblici o condivisi con altre persone, familiari compresi.

- Conosciamo le basi delle truffe e delle frodi online?
  Sapere cosa sono il phishing, i malware e altri pericoli su internet è importante per stargli alla larga.
- Proteggiamo il browser dal tracciamento online?
  Non farsi tracciare online dai siti significa bloccare la raccolta di dati. Il livello massimo di protezione e privacy su internet è la navigazione anonima. Navigare in modo completamente anonimo non è utile a tutti e non si può fare per qualsiasi situazione.
  Anche se si può navigare anonimi su internet in diversi modi, la privacy online è garantita solo con TOR browser.

Sicurezza delle password usate online

- Usiamo password complesse?
  Uno degli errori più frequenti tra i navigatori su internet è di usare password semplici o che rimandano a fatti o eventi della vita personale.
  Bisogna sempre scegliere password impossibili da scoprire e, soprattutto, generare password forti per tutti i siti web, senza dare possibilità a nessuno di poterle indovinare (mai usare la data di nascita, la squadra del cuore o il nome di un nostro caro).
- Usiamo password diverse per ogni sito?
  In nessun caso bisogna riutilizzare la stessa combinazione e-mail e password in più servizi perché se un hacker riesce ad entrare in quell'account Email, potrà violare ogni account personale senza fatica.

Sicurezza di rete

- La nostra rete Wifi di casa è protetta con chiave WPA2?
  Se non lo fosse o se non si ha idea di cosa sia WPA2, è bene consultare un tecnico specializzato per farsi configurare la rete wifi.
- Siamo consapevoli che quando ci colleghiamo ad una rete wifi aperta, tutto quello che facciamo è visibile dall'esterno del nostro computer?
  Come dimostrato, sniffare la rete e intercettare traffico internet è davvero semplice.
  L'unica cosa che protegge la sicurezza delle password su internet in una rete wifi pubblica è il protocollo HTTPS.
- Abbiamo controllato le cartelle condivise sul computer?
  Come dimostrato, entrare nei pc e vedere le cartelle condivise di altri computer è facilissimo. Molto spesso l'operazione ha successo perché ci si dimentica di levare la condivisione di cartelle o dell'intero hard disk sul computer.

Aggiornare regolarmente

Installare aggiornamenti su dispositivi, applicazioni e sistemi operativi su base regolare è un passo fondamentale per ottenere una buona igiene informatica. Sebbene sia facile ignorare gli aggiornamenti quando è necessario rispettare una scadenza o aiutare un cliente, il fatto di non mantenere aggiornati i dispositivi può semplificare drasticamente il processo per i criminali informatici che cercano di danneggiare un determinate dispositivo.

Gli accessi non si condividono, le password si scelgono con cura

La gestione degli accessi è una pratica di cyber-igiene semplice ma molto efficace. Si dovrebbero utilizzare password complesse e autenticazione a due fattori su tutti i dispositivi e gli account. Le password dovrebbero essere complesse, includendo numeri e caratteri speciali. E cercare di evitare il riutilizzo delle password attraverso vari gli account, in particolare su dispositivi e applicazioni utilizzati per accedere a informazioni aziendali sensibili. La più grande sfida per questo tipo di strategia per le password è semplicemente ricordarle o tenerne traccia. Ad esempio, è utile utilizzare acronimi o frasi per aiutare a ricordare le password.

E poiché il numero di password da ricordare aumenta, è bene prendere in considerazione l'utilizzo di software di gestione che aiutano a tenerne traccia. Le password complesse potenziate con l'autenticazione a due fattori sono ancora migliori, garantendo che solo le persone autorizzate possano accedere a sistemi aziendali sensibili e dati sensibili. I recenti progressi nella biometria, come scanner di impronte digitali e software di riconoscimento facciale, forniscono un'autenticazione a più fattori simile.

Usare l'email in maniera sicura

Il vettore di attacco maggiormente sfruttato dai cybercriminali è la posta elettronica. Normalmente, la tecnica è quelle di far cliccare i destinatari su link e allegati fraudolenti (phishing), spesso impersonando un altro dipendente o qualcuno di loro conoscenza (spear phishing).

Per combattere tali minacce, è importante essere vigili, in particolare sulle e-mail contenenti link e allegati. Anche se un'e-mail sembra provenire da una fonte attendibile, è bene assicurarsi di guardare attentamente l'indirizzo e-mail o l'URL del sito web a cui i link si riferiscono.

Installare un Anti-Malware

Mentre il software anti-malware non può fermare gli attacchi sconosciuti, la maggior parte degli attacchi e degli exploit riutilizzano gli attacchi che hanno avuto successo in precedenza. L'installazione di software anti-malware/anti-virus su tutti i propri dispositivi e reti fornisce protezione in caso di phishing o tentativo di sfruttare una vulnerabilità nota. Inoltre, è bene cercare strumenti che forniscano funzionalità di sandboxing, sia come parte di un pacchetto di sicurezza installato o come servizio basato su cloud, per rilevare anche Zero-Day e altre minacce sconosciute.

Le policy di sicurezza informatica nel GDPR

La sicurezza informatica scaturisce prima di tutto da una corretta percezione del personale e, in generale, da tutti coloro che utilizzano i servizi tecnologici messi a disposizione dalla scuola. È inutile definire policy di sicurezza IT se poi un operatore le disattende eseguendo un allegato di posta elettronica o aprendo un improbabile file, in quanto nessuno lo ha formato.

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 le workstation destinate all'uso istituzionale.

Molta attenzione, ad esempio, dovrebbe essere riposta nel

- 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 e autenticare 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 (o vietarne l'uso);
- curare l'osservanza del backup;
- evitare per l'uso di dispositivi scolastici al di fuori dell'ambito lavorativo.

La compliance al GDPR

- 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

- Implementare, attraverso uno strumento automatico, un inventario delle risorse attive
- Aggiornare l'inventario, con uno strumento automatico, quando nuovi dispositivi approvati vengono collegati in rete
- Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie
- 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.

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. Per il software non autorizzato deve esserne impedita l'installazione o l'esecuzione. Nel caso in cui, comunque, si rilevi software non autorizzato, si deve procedere immediatamente alla rimozione.
- 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.
- Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può includere i software più diffusi.

Proteggere le configurazioni di hardware e software dei dispositivi (mobili, laptop, workstation e server)

- Utilizzare configurazioni hardened (standard sicure) del dispositivo (sistema operativo, applicazioni e dati). La procedura di hardening comprende tipicamente eliminazione degli account non necessari, disattivazione o eliminazione dei servizi non necessari, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.
- Validare e aggiornare le immagini d'installazione nella loro configurazione di sicurezza, anche in considerazione delle sopraggiunte vulnerabilità e vettori di attacco.
- Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.

Valutazione e correzione continua della vulnerabilità

- Installare automaticamente le patch e gli aggiornamenti del SW per il sistema operativo e per le applicazioni.
- 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.
- 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.

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.
- 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.
- Gestire, attraverso uno strumento automatico, l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata. Va segnalata qualunque variazione.
- 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.
- Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.
- Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi.
- 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).
- 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.

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 personali.
- Limitare (eliminare) l'uso di dispositivi esterni a quelli necessari per le attività aziendali.
- Monitorare i tentativi di utilizzo di dispositivi esterni.
- Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.
- Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.

- Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione, eseguendo il content filtering del web.
- Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
- Disattivare l'esecuzione automatica dei contenuti dinamici (ad es. macro) presenti nei file.
- Disattivare l'apertura automatica dei messaggi di posta elettronica.
- Disattivare l'anteprima automatica dei contenuti dei file.
- Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.

Copie di sicurezza

- Effettuare periodicamente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema (sistema operativo, applicazioni e dati).
- 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 le copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche le 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, sul perimetro della rete, strumenti automatici per bloccare, limitare ovvero monitorare, sul traffico uscente, l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.
- 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.
- Bloccare il traffico da e verso URL presenti in una blacklist.

Le indicazioni AgID

- Un inventario hardware e software (ABSC 1.X.X e ABSC 2.X.X)
- Un sistema/processo di distribuzione delle patch di sicurezza (ABSC 3.X.X e ABSC 4.X.X)
- Un sistema di valutazione/correzione delle vulnerabilità (ABSC 4.X.X)
- Un sistema di difesa dai malware (ABSC 8.X.X.)
- Un sistema di tracciamento dei log di accesso degli amministratori di sistema (ABSC 5.X.X)
- Un sistema di filtraggio del traffico di rete e in particolare del traffico web (ABSC 8.X.X e ABSC 13.X.X)

Gli inventari

La finalità degli inventari è quella di conoscere il proprio patrimonio IT, in modo da disporre delle informazioni necessarie per gestire efficacemente le risorse e intervenire prontamente in caso di necessità. Le misure relative all'inventario prevedono anche l'individuazione di dispositivi non autorizzati (misura ALTA, al fine di identificare dispositivi che potrebbero essere portatori di minacce), così come la mappatura dei software autorizzati (in questo caso l'inventario software potrebbe essere uno strumento di controllo). Inoltre, la misura 2.3.1 prevede di eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato. L'utilizzo degli strumenti di inventario software potrebbe supportare la gestione di configurazioni standard per i dispositivi.

Il patch management

Tra i gruppi di controllo relativi alle configurazioni e quelli relativi alle vulnerabilità è trattato l'aspetto della distribuzione delle patch di sicurezza. In particolare, il controllo 4.5.1 specifica di Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.

Un sistema di valutazione/correzione delle vulnerabilità

Quando si parla di valutazione e correzione delle vulnerabilità si deve ragionare su due perimetri: il front-end, cioè l'aggiornamento costante in rete delle vulnerabilità che possono colpire i sistemi; il back-end, cioè la verifica sulla propria rete della presenza di asset che potrebbero essere vulnerabili rispetto alle minacce rilevate e l'adozione di processi correttivi.

L'aggiornamento delle vulnerabilità scoperte è auspicabile venga effettuato con strumenti automatici. Un eventuale controllo manuale, tramite consultazione di siti specifici o ricezione di newsletter, è di sua natura critico: sarebbe necessario implementare una procedura in cui si individui un soggetto che esegue giornalmente il controllo, documenti l'operazione svolta, venga previsto un suo vicario in caso di assenza… Si tratta elementi procedurali che presentano troppi punti deboli per poter garantire la sicurezza del processo.

Il sistema di protezione dai malware

Il gruppo di controllo relativo al trattamento dei malware impone di configurare i sistemi di difesa in modo da bloccare una serie di funzionalità che potrebbero attivare automaticamente delle minacce (es. apertura automatica dei messaggi di posta elettronica, anteprima dei files, ecc). Niente di nuovo, per chi gestisce una rete con consapevolezza.

Alcuni antivirus hanno affiancato alle funzionalità tradizionali delle features interessanti, come ad esempio l'inventory dinamico delle macchine su cui sono installati o la possibilità di distribuire patch di sicurezza. Caratteristiche efficaci, che vanno adeguatamente contestualizzate nello specifico ambiente che si deve gestire.

GLOSSARIO

Titolare del trattamento

- È l'Istituzione Scolastica che determina le finalità e i mezzi del trattamento di dati personali gestiti.

Responsabile (esterno) del trattamento dati

- È la persona giuridica che tratta dati personali per conto del titolare del trattamento.

Dirigente Scolastico

- È il legale rappresentate dell'Istituzione Scolastica

Responsabile Protezione Dati (RPD) o Data Protection Officer (DPO)

- È lo specialista che conosce a fondo la normativa privacy e i sistemi informatici, soprattutto dal punto di vista della sicurezza IT.

Maggiori informazioni

http://www.garanteprivacy.it (sito del Garante della Privacy Italiano)
http://www.garanteprivacy.it/regolamentoue (link diretto del Garante sul nuovo GDPR)
http://www.agid.gov.it (AGID - Agenzia per l'Italia Digitale)