Cyber Hygiene: gli ingredienti di base per un programma di cyber protection

Author : Giovanni Ciminari

Date : 2 luglio 2018

Sebbene la cultura della sicurezza del Cyber Spazio si stia (fortunatamente) diffondendo, spesso nelle discussioni tra gli addetti ai lavori a prendere il sopravvento sono tematiche assai evolute: Advanced Persistent Threat, Spear Phishing, Targeted Attack, nation-state cyber weapons, etc. Più raramente vengono presi nella dovuta considerazione gli effetti di attacchi che si basano sullo sfruttamento di vulnerabilità molto diffuse, datate e scontate: tali attacchi sono di gran lunga i più frequenti, con esiti altrettanto disastrosi rispetto ai meccanismi più sofisticati. Prendendo in considerazione il danno di immagine o gli impatti per la violazione di un regolamento vigente (ad esempio il General Data Protecion Regulation, GDPR), non è difficile immaginare come l'essere oggetto di un incidente a causa di una vulnerabilità molto banale (ad esempio la mancata applicazione di una patch di Windows o l'utilizzo di credenziali deboli sul proprio sito di e-commerce) possa essere molto più deleterio.

Non a caso, il recente rapporto del National Cyber Security Center "The cyber threat to UK business "2017-2018, stigmatizza l'alta diffusione di software non patchato nel sistema pubblico e privato in UK: "**highlighting the importance of basic security practices".**

Potremmo dire che un programma completo di cyber security può essere rappresentato come una costruzione con delle fondamenta (pratiche di base di security e di corretta gestione degli asset) e con un piano rialzato composto dalle soluzioni tecnologicamente più evolute (IPS, WAF, NAC, anti APT, EDR, Risk Based authentication,…): la solidità del piano dipende dalle sue fondamenta.

Fanno parte delle pratiche di base: le tecniche di Hardening, il Patching, la segmentazione della Rete, la sicurezza dei protocolli e la sicurezza delle credenziali di autenticazione. Tali elementi vengono comunemente racchiusi nel concetto di **Cyber Hygiene**.

Nello specifico:

- le tecniche di Hardening contribuiscono a mantenere una elevata sicurezza di base

delle apparecchiature, da cui vengono rimossi i comandi e i servizi non indispensabili e più soggetti ad un utilizzo malevolo;
- una politica periodica di Patching garantisce di avere a disposizione sempre la versione più aggiornata del software (contenente quindi tutte le fix di sicurezza) per la versione di prodotto che si utilizza;
- la segmentazione della Rete contribuisce ad isolare le apparecchiature rivolte verso il mondo esterno (Internet) dai legacy aziendali, le applicazioni aziendalmente più critiche da quelle che lo sono meno, riducendo quindi l'esposizione di infrastrutture e dati al minimo necessario;
- è una doverosa pratica di sicurezza non solo l'adozione di protocolli di comunicazione sicuri, autenticati e cifrati(anche nelle comunicazioni tra apparecchiature interne all'azienda) ma anche l'adozione di credenziali di autenticazione che si adattino al contesto di utilizzo che può richiedere una semplice password (in questo caso verificando che le regole di composizione e sostituzione periodica siano in linea con le policy aziendali o con le best practice in materia) fino a eventuali meccanismi basati sul riconoscimento biometrico.

Se ci fosse bisogno di rimarcare l'importanza di queste pratiche, basterebbe ricordare come la minaccia che ha avuto la maggiore risonanza nel 2017 in tutto il mondo, **Wannacry**, non sia altro che una questione di Cyber Hygiene: le aziende più efficaci nelle pratiche di patching del proprio sistema informativo, che avevano installato il software che correggeva la vulnerabilità descritta nel CVE-2017-0144, non hanno subito alcun impatto sul proprio business.

Cyber Hygiene

Per Cyber-Hygiene si intende quindi una serie di principi, semplici ma efficaci, che devono essere osservati quotidianamente per minimizzare, e se possibile azzerare, il livello di rischio residuo delle applicazioni aziendali. La questione rilevante è che, pur essendo i principi di base semplici, molto spesso non è tale la loro applicazione in sistemi informativi complessi.

La disciplina del Cyber Hygiene si articola in tre fasi: planning, execution e check.

Nella fase di planning è essenziale:

- determinare l'insieme degli asset che compongono il sistema informativo,
- identificare le regole di hardening ed un processo per il loro aggiornamento,
- identificare il processo di verifica del patching (frequenza, prodotti interessati, possibili impatti),
- definire un modello di segmentazione (nord/sud, est/ovest) in base ai principi di analisi del rischio adottati,
- stilare la lista dei protocolli classificati come sicuri e le loro caratteristiche (es. mutua autenticazione), i metodi di autenticazione ammessi e i criteri di accettazione delle credenziali (es. dizionario dei termini da escludere).

Nella fase di execution gli elementi rilevanti riguardano soprattutto patching e hardening, che possono impattare sui sistemi in produzione: le normali precauzioni in questo caso prevedono di

operare dapprima in ambiente di pre-produzione per gestire in sicurezza eventuali incompatibilità.

Nella fase di check è importante essere in grado di verificare in maniera oggettiva e aggiornabile il corretto stato di Cyber Hygiene. In tal senso, operare in maniera automatizzata garantisce sia la riproducibilità che la possibilità di eseguire verifiche molto frequenti lasciando quindi una finestra di esposizione al rischio ridotta rispetto all'insorgere di una nuova vulnerabilità.

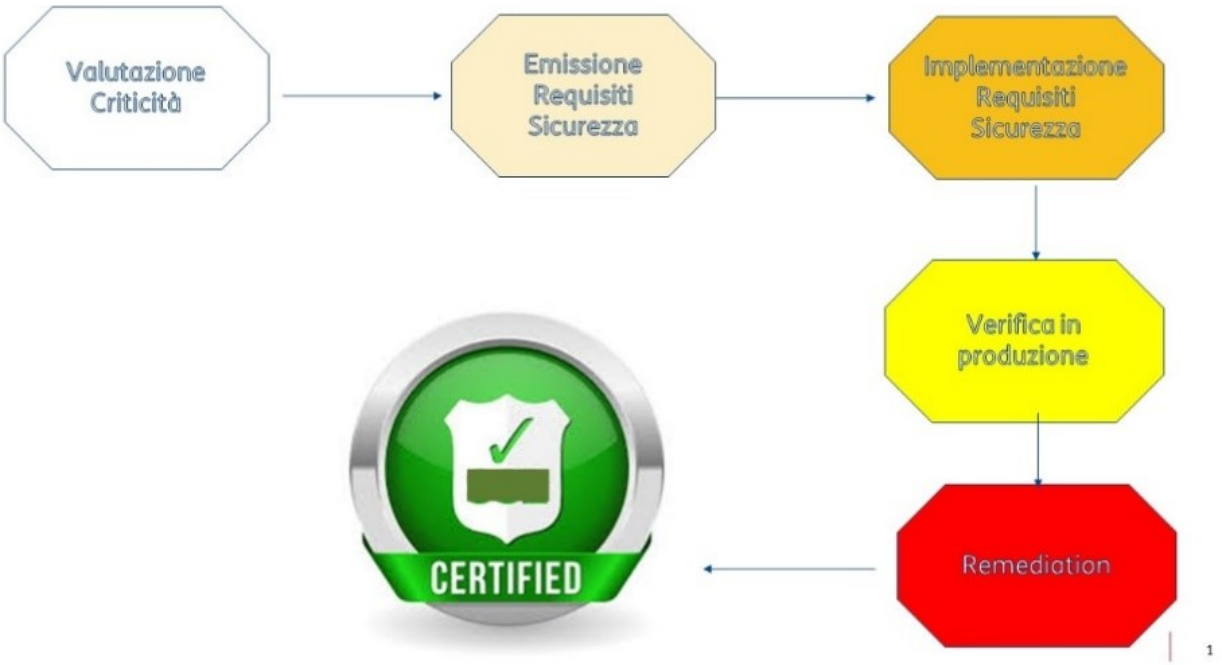
In aziende di medio-grandi dimensioni implementare e mantenere un processo che garantisca un adeguato livello di Cyber Hygiene è estremamente sfidante: nel caso di centinaia o migliaia di server i controlli da dover implementare potrebbero essere migliaia e con decine di varianti e peculiarità (considerando che i requisiti da applicare variano a seconda degli strati software quali sistema operativo, middleware e applicazioni).

Per questo motivo è auspicabile poter contare su una **piattaforma specializzata** in grado di automatizzare sia la fase di planning che quella di check. Per la fase di execution sono le piattaforme commerciali di System & Network management a poter fornire un valido aiuto.

Cyber Hygiene "automatizzata"

Dall'esperienza di una grande realtà industriale come TIM, è nata una piattaforma di supporto al processo di mantenimento della Cyber Hygiene. Tale piattaforma, composta da vari moduli, prevede il supporto sia alla fase di planning (mediante un cruscotto) che alla fase di check mediante alcuni strumenti di verifica verso i sistemi target.

Il cruscotto si alimenta con i dati delle applicazioni sulle quali viene preventivamente effettuata un'analisi di sicurezza che, in base al livello di criticità assegnato, guida la definizione dei requisiti di sicurezza da applicare. Il problema, ora è verificare l'effettiva adozione di tali requisiti.



Il processo che dalla definizione dei requisiti alla certificazione dell'implementazione sostiene la Cyber Hygiene

Tutte le informazioni relative alla Cyber-Hygiene confluiscono in un cruscotto manageriale integrato con uno strumento di Business Intelligence che consente di avere in un unico colpo d'occhio la situazione sullo stato del processo. Navigando fra le diverse applicazioni o sulle vulnerabilità è possibile approfondire l'analisi fino ad arrivare ad evidenziare l'elenco delle vulnerabilità di un unico host oppure l'elenco degli host affetti da una unica vulnerabilità. Mediante lo strumento vengono effettuate analisi temporali in modo da valutare i KPI (Key Performance Indicator) stabiliti, quali ad esempio il numero di non conformità rispetto alla numerosità degli asset.

Il processo di analisi delle vulnerabilità delle applicazioni è per sua natura ricorsivo: lo strumento arricchendosi periodicamente con i dati delle scansioni più recenti è in grado di mostrare la serie storica delle vulnerabilità ed è possibile visualizzare il "percorso" di sicurizzazione compiuto su una o più applicazioni aziendali a seguito degli interventi di 'remediation' eseguiti.

Alcune tipologie di requisiti possono essere indirizzati attraverso soluzioni aziendali centralizzate (ad es. AAA-Autenticazione, Autorizzazione ed Accounting). Altri requisiti, come ad es. l'Hardening ed il Patching, rispondono a delle linee guida che devono essere applicate a cura dell'owner (gestore) dell'applicazione.

La fase di check può quindi seguire diversi percorsi, dalla verifica sul sistema di CMDB (Configuration Management Data Base), all'interrogazione delle soluzioni di sicurezza aziendali

(es. IAM, Active Directory, …) laddove la verifica di una effettiva integrazione corrisponde al superamento del requisito, all'accesso diretto alle applicazioni sia dall'esterno che dall'interno (scansioni non autenticate e scansioni autenticate). Purtroppo non tutti i controlli che assicurano una corretta Cyber Hygiene sono automatizzabili: una percentuale non trascurabile richiede l'intervento di una analista che con il proprio know-how sia in grado di stabilire che il requisito sia correttamente e quindi efficacemente implementato.

Vediamo di seguito una rassegna dei controlli automatizzati.

Patching check

Un meccanismo alternativo all'utilizzo del CMDB per identificare l'aggiornamento o meno del software è l'utilizzo di uno strumento di Vulnerability Assessment (ad es. Nessus). Questo meccanismo consente di effettuare verifiche su qualunque tipologia di server, indipendentemente dal sistema operativo, ed è sufficiente definire un elenco di "plugin", racchiusi in una policy di scansione, per ricercare l'elenco dei prodotti vulnerabili installati, indicandone la vulnerabilità e la contromisura di sicurezza raccomandata.

Tali verifiche raggiungono il massimo grado di affidabilità se vengono effettuate in modalità "white-box", utilizzando un account con adeguato livello di privilegi già presente sul server. In modalità black-box invece, quando la scansione viene effettuata senza accedere al server, vengono effettuati dei tentativi di rilevazione dei software installati, ad es. dai banner di accesso o verificando le porte standard dei protocolli più comuni.

Hardening check

Le linee guida di hardening vengono definite e applicate sui sistemi su indicazione dell'owner dell'applicazione, che deve armonizzare tali linee guida preservando il corretto funzionamento senza intaccarne la validità in termini di security.

L'applicazione viene quindi sottoposta periodicamente alla verifica di implementazione dell'hardening, mediante strumenti automatici che si connettono direttamente ai server e verificano i singoli item attestandone l'effettiva applicazione.

Password check

Le credenziali di accesso predicibili rappresentano un fattore di rischio molto elevato per cui è necessario adottare password policy stringenti e verificarne l'effettiva adozione. Uno dei metodi più efficaci per effettuare questa verifica è "Hashcracking".

Tale tecnica enumera gli account presenti in un determinato contesto (ad es. gli utenti di sistema operativo), estrae l'hash della password e lo confronta con un dizionario di password deboli composto da decine di milioni di termini, al fine di evidenziare eventuali password predicibili.

Specchietto esemplificativo sui tempi di decodifica di alcune tecniche di hashing (Scenario: 4 GPU Nvidia, 62mln di entry, password non crackata):

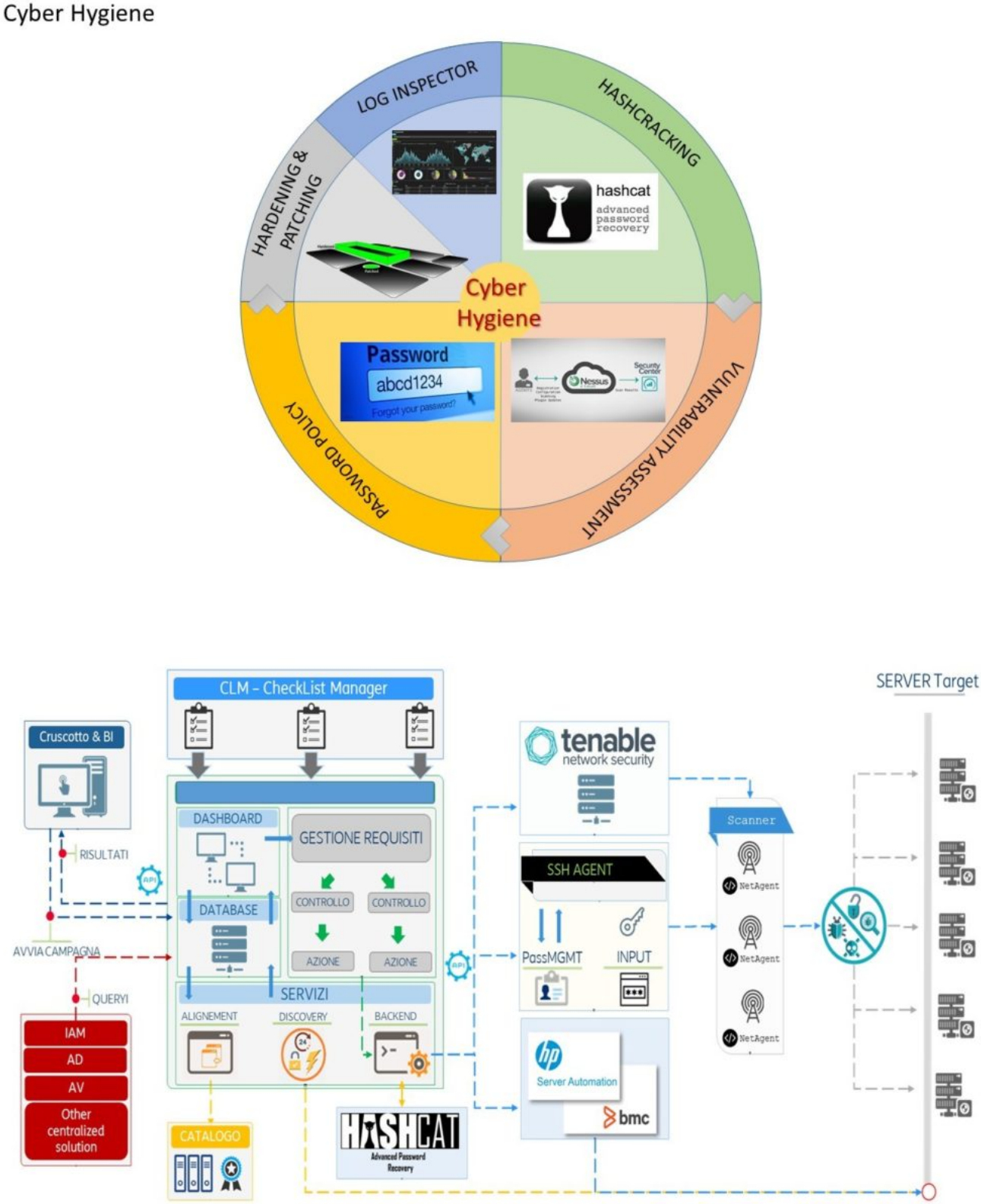
Num. Hash	descrypt	md5crypt	sha512crypt	bcrypt [5]	bcrypt [10]
1	6 sec	24 sec	38 min	6,5 ore	9 gg
10	55 sec	4 min	6 ore	2,8 gg	3 mesi
20	2 min	8 min	12 ore	5,4 gg	6 mesi
40	4 min	16 min	24 ore	10,8 gg	1 anno

Il tempo richiesto dal processo di Hashcracking è funzione dell'algoritmo di hash utilizzato e della potenza elaborativa a disposizione. Per aumentare quest'ultima grandezza vengono utilizzati dei supporti hardware basati su GPU (Graphics Processing Unit) in grado di garantire un alto parallelismo di calcolo.

Log Inspector

L'analisi automatica e a posteriori dei log di accesso ai sistemi ed alle applicazioni, c.d. Log Inspecting, è una efficace tecnica di Cyber-Hygiene perché, incrociando i dati degli accessi rilevati dai log con gli elenchi degli utenti autorizzati e le matrici dei profili ad essi associati, consente di verificare che i meccanismi di sicurezza degli accessi siano correttamente configurati e funzionanti e di rilevare eventuali accessi non consentiti.

Una analisi massiva (non personalizzata) e continua dei dati relativi ai dati di tracciamento, eventualmente analizzata con tecniche di Machine Learning, consente di rilevare eventuali scostamenti, nei volumi e nei contenuti, che possono fornire una indicazione di variazione (ad es. una applicazione che non invia più dati di tracciamento oppure che ha variato il formato) su cui avviare i necessari approfondimenti.



Architettura di riferimento per l'automazione dei controlli di Cyber Hygiene

Estensione del perimetro agli apparati di rete

In un contesto quale quello di un operatore di telecomunicazioni, inoltre, è essenziale poter estendere i principi della Cyber Hygiene anche agli apparati di rete. Con lo stesso cruscotto con cui si analizza il sistema informativo, potranno quindi essere raccolti i dati sulla corretta configurazione di migliaia di CPE (Customer Premises Equipment) per verificare la loro corretta configurazione (eliminazione servizi inutili, raggiungibilità da internet, corretta attivazione del servizio di AAA), l'adeguatezza della versione di hardware e software.

Conclusioni

Implementare un processo che garantisca un corretto percorso di Cyber Hygiene è certamente un obiettivo basilare di un efficace strategia di protezione aziendale.

In realtà complesse, garantire la Cyber Hygiene significa pianificare e verificare decine di migliaia di controlli. L'adozione di strumenti automatici e di una vera e propria piattaforma di gestione consente di:

- rendere riproducibili ed esenti da errori operativi i risultati
- ridurre i costi e i tempi di esecuzione
- capitalizzare il know-how del personale specialistico in un momento di significativa carenza di skill tecnici, in particolare di Cyber Security
- poter disporre di informazioni sullo stato di salute del proprio ambiente IT in tempi brevissimi, con dati oggettivi e monitorabili nel tempo (trend storici) mediante la definizione di opportuni KPI.

Come riportato nell'articolo, la Cyber Hygiene è un processo continuativo e quindi sempre migliorabile lungo le direttrici di una sempre maggiore copertura, automatizzazione ed efficacia del singolo controllo.

A cura di: **Giovanni Ciminari** e **Angelo De Spagnolis**