Web security: rendere Internet un luogo sicuro

La “web security” è sempre più necessaria per garantire una navigazione web sicura

La “web security” è una parte della “Internet security” sempre più necessaria per garantire la navigazione web all’interno di Aziende, Organizzazioni e Scuole di ogni ordine e grado, al fine di lavorare in tranquillità da minacce e contenuti indesiderati. Una “cyber security solution” efficace richiede quindi un insieme di tecnologie, di procedure e di mezzi dedicati alla protezione dei sistemi informatici.

1. Cos’è la Web Security?

Il web è una fonte illimitata di informazioni e risorse di ogni genere, usufruibile da chiunque in maniera semplice ed intuitiva, quindi è di notevole importanza essere coscienti ed informati su quelli che possono essere i pericoli presenti nel mondo di Internet.

Si stima che **nei prossimi 2/3 anni, quasi il 100% di tutto il carico di lavoro verrà spostato sul Cloud**, quindi la web security assume ancor di più un ruolo fondamentale in aziende, organizzazioni e scuole di ogni ordine e grado.

La **web security** si occupa di fornire gli strumenti, le procedure e le varie regole utili al fine di proteggere sé stessi e la propria infrastruttura da attacchi informatici,

perdita di dati e dall'accesso a siti pericolosi o indesiderati. Molto spesso si tende a trascurare il concetto di internet security pensando di essere immuni o di non essere oggetti potenziali di estorsioni informatiche o tentativi di furto dei dati, ma non è così in quanto gli attacchi molto spesso vengono fatti anche solo per danneggiare la reputazione o rallentare l'operatività di un'impresa, di un'organizzazione o di un istituto.

Si rischia tutti i giorni in quanto anche **una minima interruzione o violazione della sicurezza in Rete può comportare innumerevoli perdite di tempo e di dati**, ritardi, disservizi ai propri clienti e quindi danneggiare i profitti e la credibilità aziendale.

Negli ultimi anni sono sempre di più le Organizzazioni costrette a chiudere in seguito a grosse perdite di dati e/o al pagamento di ingenti riscatti per non rendere pubblici dati e informazioni sensibili, o infine a causa di ricatti da parte di hacker che hanno paralizzato l'attività aziendale.

Vediamo allora quali sono i principali interventi da tenere in considerazione quando si parla di "Web security" (o sicurezza di rete).

1.1 Formazione sulla web security

La sicurezza parte innanzitutto dalla formazione dei vari utenti della rete, al fine di fornire una serie di regole e standard da seguire per mantenere il proprio network protetto e garantire una **navigazione web protetta**.

È necessario informare periodicamente i membri della propria organizzazione sulle varie procedure di web security da seguire per evitare di compromettere il proprio lavoro e quello degli altri utenti della rete, inoltre, è importante mantenere le proprie credenziali private e non accessibili/visibili da terzi.

La maggior parte degli attacchi informatici avvengono a seguito di errori umani, dovuti spesso alla poca formazione e attenzione durante le normali attività lavorative: ad esempio l'apertura di allegati, come file Excel o Word, arrivati tramite email e che

possono comportare grossi pericoli non solo per i propri dati ma per tutta la rete aziendale.

La verifica della fonte (mittente) prima di scaricare/aprire allegati o link presenti nel testo del messaggio è un passaggio essenziale e per questo esistono i **Cryptolocker** che hanno lo scopo di criptare tutti i dati presenti nella propria macchina, bloccando l'apertura e rendendoli inutilizzabili. Questi attacchi non si fermano molto spesso alla singola macchina ma si diffondono molto rapidamente su tutta la rete e sui vari percorsi condivisi, criptando così i dati anche degli altri utenti della rete.

Arriviamo quindi ad un altro strumento fondamentale per evitare la perdita di dati e informazioni, ovvero i backup. Mantenere un **sistema di backup** che permetta di memorizzare i propri dati su dispositivi esterni (o sul Cloud), è oggigiorno un **elemento importantissimo al fine di evitare ingenti danni** che, in diversi casi, hanno comportato anche la chiusura dell'attività stessa.

Un'altra regola da tener presente quando si parla di sicurezza (in questo caso si fa riferimento alla sicurezza della rete aziendale piuttosto che web), è quello di bloccare agli utenti l'utilizzo di chiavetta USB o dispositivi di memorizzazione esterni (come dischi esterni o CD/DVD), dal momento che virus/malware possono essere facilmente trasferiti da un dispositivo ad un altro semplicemente collegandolo alla propria macchina.
È doveroso utilizzare **password che rispettino i requisiti minimi di complessità** e configurare regole per il cambio della password almeno ogni 6 mesi.

1.2 L'importanza (anche) del Software Antivirus

Un altro aspetto molto importante è l'utilizzo di un **software Antivirus** installato su ogni dispositivo di rete. Lo strumento in grado di **garantire protezione e sicurezza al proprio dispositivo** (e alla rete stessa), è proprio l'Antivirus.

L'Antivirus è in grado di bloccare una possibile minaccia come, ad esempio, un Malware/Trojan.
Bisogna ricordarsi però che molto spesso non basta digitare sul web "miglior antivirus free" ed installarlo nella propria rete per ottenere un buon livello di sicurezza. È infatti necessario mantenere sempre il prodotto aggiornato sia a livello di database dei virus sia a livello di patch di sicurezza, eseguire inoltre scansioni periodiche al fine di eliminare file/cartelle potenzialmente pericolose.

2. Filtro per contenuti web

Per quanto concerne la "web security", un fattore molto importante da tenere in considerazione riguarda l'applicazione di **un filtro contenuti in grado di bloccare l'accesso a siti e risorse web potenzionalmente pericolose o indesiderate**. Quando apriamo un sito (per esempio google.com) il nostro Browser, per prima cosa traduce l'URL in un indirizzo IP pubblico, univoco nella rete, al fine di instradare il traffico verso la risorsa cercata.

Questo processo di assegnazione dei nomi ai nodi della Rete (host) viene fatto attraverso un sistema molto complesso, denominato DNS (Domain Name System). **La risoluzione DNS** indica il procedimento di conversione da nome ad indirizzi IP, e quindi con il termine DNS si intende anche il protocollo stesso che consente tale operazione.
I filtri più professionali lavorano a **livello DNS**, analizzando la richiesta del Cliente e, in base a regole pre-configurate, bloccando o consentendo l'accesso al sito (o risorsa) desiderato.

FlashStart, ad esempio, è un player globale che offre un robusto servizio di **filtraggio DNS**, semplice ed intuitivo, che permette ai clienti di mettere in sicurezza la propria rete in tempi brevi e senza la necessità di acquistare/installare ulteriore hardware.

In aggiunta, visto che lo smart working è sempre più comune nella nostra vita, FlashStart fornisce anche una possibilità molto importante, ossia quella di proteggere i dispositivi personali tramite l'installazione di un'app. In questo modo sarà garantita

la “web security” anche all’utente connesso da remoto, evitando l’accesso a siti indesiderati o potenzialmente pericolosi. Ciò è importantissimo perché **molti attacchi hacker recentemente hanno colpito le aziende entrando tramite i lavoratori a distanza**.

Oltre a garantire la web security, i filtri hanno anche lo scopo di limitare l’accesso degli utenti a siti e applicazioni che potrebbero compromettere la produttività, evitando quindi perdite di tempo in orario lavorativo. Parlando nuovamente di FlashStart, la sua **Dashboard permette di bloccare, oltre ai siti infetti e ai contenuti espliciti, anche l’apertura di siti di svago, Social Network, giochi online e altri servizi che porterebbero a rallentamenti sulla produttività aziendale**.

La piattaforma è configurabile **con oltre 85 Blacklist internazionali aggiornate continuamente grazie all’intelligenza artificiale,** dispone della granularità per utenti e gruppi, dell’integrazione con sistemi di terze parti (API), policy per fasce orarie,. Fra l’altro FlashStart propone un filtro Cloud compatibile con tutti i dispositivi di Router, WiFi Hotspot, Firewall, Gateway presenti in circolazione.

Oltre a quelle elencate sopra possono essere molto utili queste funzionalità aggiuntive:

» Protezione delle ricerche di Google/Bing tramite **Safesearch**, con filtro delle immagini integrato

» Protezione di Youtube, bloccando la visualizzazione di video non adatti ai minori

» Configurazione della propria pagina di blocco, con tanto di logo e testo personalizzati

» **Geoblocking**: blocco di siti e risorse a livello geografico

» Applicazione delle regole di filtro in base al singolo dispositivo (o utente/gruppo di Active Directory)

» Protezione dei dispositivi mobile tramite l’installazione di un app

» Invio automatico di report estremamente dettagliati tramite email

» Analisi del traffico sia in tempo reale (per debug) sia quello transitato in una determinata giornata

3. Web security tramite Rete perimetrale

Uno degli elementi di maggior importanza nell'ambito della web security è rappresentato dal **Firewall** di rete. Il **Firewall** **più semplice deve consentire il blocco di porte/servizi in uscita ed in particolar modo in entrata**, consentire all'utente la visualizzazione del proprio traffico di rete (ad esempio a scopo di debug) e introdurre sistemi per la separazione fisica (o virtuale tramite VLAN) delle reti interne.

Oggigiorno esistono **Firewall** in grado di svolgere anche attività complesse come:
» **IPS** (Intrusion Prevention System): permette di analizzare il traffico con lo scopo di segnalare e/o bloccare attività dannose.
» **Filtri Layer 7**: Permotto di bloccare le applicazioni indesiderate o che possono comportare grossi rallentamenti sulla rete (esempio Torrent e peer to peer)
» **Prevenzione e blocco di accessi non autorizzati al sistema** (esempio tentativi di accesso al Firewall in SSH o da portale web)
» **Filtri antispam**: Analisi della posta con la possibilità di bloccare la posta indesiderata
» **VPN e telelavoro**: Creazione e gestione di VPN per connettere due o più sedi remote o per collegarsi da remoto in smart working.
Produttori e installatori di Firewall intervengono nella web security soprattutto a livello perimetrale ma ciò non è completo né a livello di protezione né a livello di aggiornamento.
FlashStart ha recentemente rilasciato un'estensione della protezione in Cloud chiamata **Hybrid Firewall**, con lo scopo di integrare tutte le principali funzioni svolte da un Firewall con i suoi filtri Cloud continuamente aggiornati da un'Intelligenza Artificiale.

Tra le varie funzioni presenti su **Hybrid Firewall**, si ha la possibilità di creare diversi profili di navigazione, associando quindi regole (filtri) diversi in base all'utente/gruppo (se presente un Server di Dominio con ruolo di Active Directory) o all'IP privato che ha fatto la richiesta. Rispetto alla soluzione Cloud, per utilizzare **Hybrid Firewall** è

necessario acquistare un hardware apposito (o utilizzare un proprio dispositivo che rispetti le caratteristiche tipiche del prodotto).

4. Scegliere una giusta Web Security

FlashStart, azienda europea presente su scala globale, propone una soluzione di web filter molto apprezzata per garantire una internet security universale. FlashStart ha a disposizione una **Rete Anycast** di datacenter in diverse aree geografiche e ha clienti in più di 145 Paesi.

Come quasi tutte le soluzioni, il filtro di FlashStart agisce sul **protocollo DNS**, individua e blocca i malware, garantisce un database sempre aggiornato e una reportistica completa.
Importanti caratteristiche distintive di FlashStart sono il **geoblocking**, ovvero il blocco all'accesso a siti in determinate aree geografiche, e il blocco a tempo, ovvero impostato su un intervallo di tempo ben preciso. Ciò permette, per esempio, l'accesso ai social network, in orari diversi da quello di lavoro.

Infine, **da segnalare l'integrazione con Microsoft Active Directory, non presente in tutti i vendor di soluzioni simili, e il supporto garantito 24/7 in italiano, inglese e spagnolo**.
Ancora, FlashStart permette anche di estendere la protezione agli end point remoti, come i computer portatli, i tablet e gli smartphone. Da sottolineare, inoltre, che FlashStart lavora solo con rivenditori e offre ai partner che si distinguono per performance, **margini che possono arrivare oltre al 60% del prezzo di vendita finale**, ossia più del doppio rispetto ai guadagni consentiti dai competitor.