PROTOCOALE DE SECURITATE

Gabriel – Cătălin STĂNESCU,
Facultatea de Matematică si Informatică

CZU: 004.056 *darkside_1ro@yahoo.com*

Internetul nu a fost creat cu gândul la securitate. Scopul lui inițial a fost conectarea persoanelor fără a tine cont de barierele fizice. Bineînțeles că nu toți utilizatorii au scopuri oneste, și, de aici, a apărut nevoia securizării datelor transmise prin rețeaua globală.

Cu toții dorim ca atunci când suntem online să fim in siguranță, să putem purta o conversație, să putem partaja informații cu un partener fără ca altcineva să „asculte" sau să intervină.

Cum putem folosi internetul pentru a comunica sigur cu partenerul nostru? O soluție ar fi să cream un canal de comunicare criptat intre sursă și destinație. Cu alte cuvinte, putem folosi infrastructura internetului ca și cum ar fi o conexiune locală.

Tehnologiile VPN pot folosi, pentru a implementa securitatea, una din două tehnologii, sau ambele: Internet Protocol Security denumit IPsec sau Secure Sockets Layer, SSL. Ca o mică paranteză, tehnologia SSL a fost înlocuită de Transport Layer Security (TLS) dar in continuare se folosește denumirea de SSL si uneori cea de SSL/TLS.

Ambele tehnologii asigura Confidențialitatea, Integritatea și Autenticitatea comunicațiilor dar sunt unele diferențe notabile in modul lor de implementare, puncte forte și cazuri de utilizare.

Prima diferență este nivelul in care acestea activează: vorbind in contextul Modelului OSI, IPSec este o suită de protocoale de nivelul 3 (Network) pe când SSL este un protocol de nivel 6 (Presentation). De aici vine și următoarea deosebire: pe când IPsec necesita o aplicație client care sa gestioneze conexiunea, SSL nu are nevoie decât de un browser care suportă aceasta tehnologie. In concluzie, configurarea IPsec este mai complexă pe când SSL, in principiu, pentru un user obișnuit nu trebuie configurat.

Folosind IPsec, din punct de vedere al utilizatorului, el este direct conectat la rețeaua de la birou. In schimb, utilizatorul de SSL accesează doar anumite servicii făcute publice de serverul de la birou, prin browser, deci acțiunile pe care acesta le poate face sunt limitate, in contrast cu utilizatorul de IPsec care are acces total la rețea. Aici pot apărea discuții cu privire la securitate, cum că e mai sigur să dai acces doar la anumite resurse și nu la toată rețeaua. Cu toate acestea, ambele folosesc metode similare de protecție a datelor.

Observând diferențele, deja ne putem da seama de anumite cazuri de utilizare, când poți să folosești o tehnologie sau alta, când una e mai avantajoasă ca cealaltă.

Pentru a conecta două sedii ale unei societăți mai mult ca sigur vei apela la suita de protocoale IPsec. Dacă doar dorești să dai acces angajaților care lucrează „remote" la unele resurse de pe serverele firmei, atunci vei folosi SSL.

Am specificat ca IPsec se foloseste de obicei pentru mediul enterprise, pentru comunicarea diferitelor brach-office intre ele. Aceasta suita de protocoale poate fi folosita si pentru conexiune „host to network" dar poate fi anevoioasa si de cele mai multe ori nu se poate configura. Negocierea tunelului securizat presupune accesul la configurarea ambelor routere care comunica si acest lucru nu este posibil mereu. Pentru routerul de intrare in reteaua societatii nu ar fi o problema, dar pentru accesul la routerul unui hotel unde este cazat angajatul nostru, asta e problematic.

In concluzie, folosirea tehnologiei VPN in combinatie cu protocoalele de securitate amintite, confera posibilitatea comunicarii sigure in mediul online.

Bineinteles ca aceste tehnologii sunt intr-o permanenta modificare si imbunatatire pentru a tine pasul cu inventivitatea hackerilor si exploatarea vulnerabilitatilor.

Chiar daca sunt implementate protocoale de securitate, nu inseamna ca trebuie sa ne bazam strict pe ele, ci trebuie sa fim constienti si de rolul factorului uman in asigurarea confidentialitatii si integritatii datelor.

Referințe:

1. Cisco Networking Academy Builds IT Skills & Education For Future Careers (netacad.com).

2. Domantas G. https://www.hostinger.com/tutorials/what-is-ssl-tls-https.
3. IPsec (Internet Protocol Security) (networklessons.com).

Recomandat
Maria CAPCELEA, dr., conf. univ.