Razmjena povjerljivih podataka putem interneta sigurnosnim protokolima i način spajanja s interneta na intranet

Kujundžić, Mario

VELEUČILIŠTE

s pravom javnosti

BALTAZAR ZAPREŠIĆ

Zaprešić

Preddiplomski stručni studij

Informacijske tehnologije

MARIO KUJUNDŽIĆ

Razmjena povjerljivih podataka putem interneta sigurnosnim protokolima i način spajanja s interneta na intranet

PREDDIPLOMSKI ZAVRŠNI RAD

Zaprešić, 2022. godine

VELEUČILIŠTE

s pravom javnosti

BALTAZAR ZAPREŠIĆ

Zaprešić

Preddiplomski stručni studij

Informacijske tehnologije

PREDDIPLOMSKI ZAVRŠNI RAD

Razmjena povjerljivih podataka putem interneta sigurnosnim protokolima i način spajanja s interneta na intranet

Mentor:

doc. dr. sc. Matija Varga, viši znanstveni suradnik

Naziv kolegija:

INFORMACIJSKE TEHNOLOGIJE

Student:

Mario Kujundžić

JMBAG studenta:

0234060101

Sadržaj

Sažetak

Kako bismo osigurali siguran i kontroliran način prijenosa povjerljivih podataka između dva računala na različitim lokacijama, potrebno je svaki segment OSI slojevne strukture pravilno procesuirati kako ne bi došlo do „curenja“ podataka u samom prijenosu istih.
Naravno, da bismo ispunili uvjete nekog poduzeća za slanje njihovih podataka prema drugim komitentima, moramo se pridržavati nekih sigurnostih protokola koje samo poduzeće uvjetuje da bi se sklopio ugovor o radu suradnji.
Prilikom dogovora i konfiguriranja načina spajanja, potrebno je definirati kolika je razina sigurnosti potrebna da bi se miniminalni uvjeti zadovoljili što se tiče samog prijenosa podataka s lokalne na javnu mrežu.

Summary

In order to ensure a secure and controlled way of transmitting confidential data between two computers at different locations, each segment of the OSI layered structure needs to be processed properly so as not to leak the data in the transmission itself.
Of course, in order to be eligible for a company to send their data to other agents, we need to adhere to some of the security protocols imposed by the company itself in order to enter into a cooperative employment contract.
When agreeing and configuring the means of connection, it is necessary to define the level of security required to meet the minimum requirements as regards the mere transmission of data from the local to the public network.

Uvod

Dolaskom novih tehnologija, dolaze i novi troškovi za nadogradnju postojećeg IS (U nastavku rada, informacijskog sustava) kako bi neko poduzeće bilo u korak s vremenom i radilo s najnovijom tehnologijom koja je nadogradiva, dostupna za većine novih sustava i računala.
Kako dolaze nova ažuriranje, sustavi, windowsi, programi za spajanja na nečije interne mreže, tako i s tim dolaze novi propusti u samom spajanju i potencijalna opasnost za korisnike istih zbog proboja u sam sustav.
Spriječavanje hakerskih napada iziskuje stalno unapređivanje sustava kojim se koristi neko poduzeće.
U nekim poduzećima, korisnici se služe razmjenom podataka nego jednostavnim pretraživanjem interneta i slanjem elektroničke pošte, gdje se jedino elektronička pošte može presresti i ukrasti podatke, no ni to nije opasno ako se kroz elektroničku poštu šalju samo neformalne poruke koje nisu povjerljive.
No, neka poduzeća, kao što su računovodstvena i knjigovodstvena poduzeća, iziskuju najvišu razinu sigurnosti što se tiče slanja podataka putem interneta.
Kada se radi o takvom poduzeću, vrlo je bitno da se podaci koje smiju vidjeti samo stranke i firme čija se financijska izvješća ili recimo, plaće, budu obrađene s jedne strane i direktno, bez ikakvog posrednika u transportnom sloju OSI-a budu poslane ka primatelju.
Ovdje nastupaju razni protokoli za spajanje s lokalne mreže na javnu, propuštanje portova (port forward), VPN (Virtual Private Network).
Svaki od protokola i načina spajanja ima svoje mane i vrline te svrhu u različitim situacijama.
Samim time, i oni s lošim namjerama pronalaze razne načine kako probiti jedan takav protokol ili sigurnosno spajanje sa na primjer, dvofaktorskom autentikacijom koja se počela koristiti u mnoge svrhe baš zbog raznih napada na velike tvrtke.

Pojmovnik

Uvod u pojmovnik

U ovom dijelu ćemo elaborirati pojmove vezane za načine spajanja i sve sigurnosne protokole koje ćemo spominjati u nastavku ovog rada.

TCP/UDP Protokol

Tcp

protokol

Oba navedena protokola služe za slanje bitova putem mreže, no svaki za sebe ima jednu bitnu razliku. TCP protokol je najčešće korišten protokol te je specifičan po tome što se oslanja na pouzdanost, odnosno, provjerava i čeka odgovor s druge strane je li paket stigao s nekim gubitkom bitova ili je u potpunosti primljen kako je i poslan.
Koristi se kod procesa koji iziskuju pouzdanost i neku vrstu sigurnosti, kao što je na primjer email, povezivanje na neke druge mreže…

Udp protokol

Ovaj protokol je suprotnost TCP protokolu, odnosno, on se veže na brzinu te kada izvrši slanje podataka, ne čeka povratnu informaciju je li bit odnosno paket stigao u cijelosti ili se dogodila latencija i gubitak djelića paketa. Najčešće je korišten kod nekakve vrste streaminga odnosno reproduciranja videa ili zvuka gdje ako se i desi gubitak dijela podataka, on nastavlja dalje odnosno smanji kvalitetu zapisa. Često je korišten i kod DNS servera gdje je bitna zapravo brzina sinkroniziranja servera s računalima (Clusters).

Ova dva protokola se nalaze u transportnom OSI sloju te su vrlo važni za slanje i primanje podataka.

DNS

Domain name system je sustav koji upravlja dodjeljivanjem imena za servere, računala i sve uređaje koji koriste mrežu.

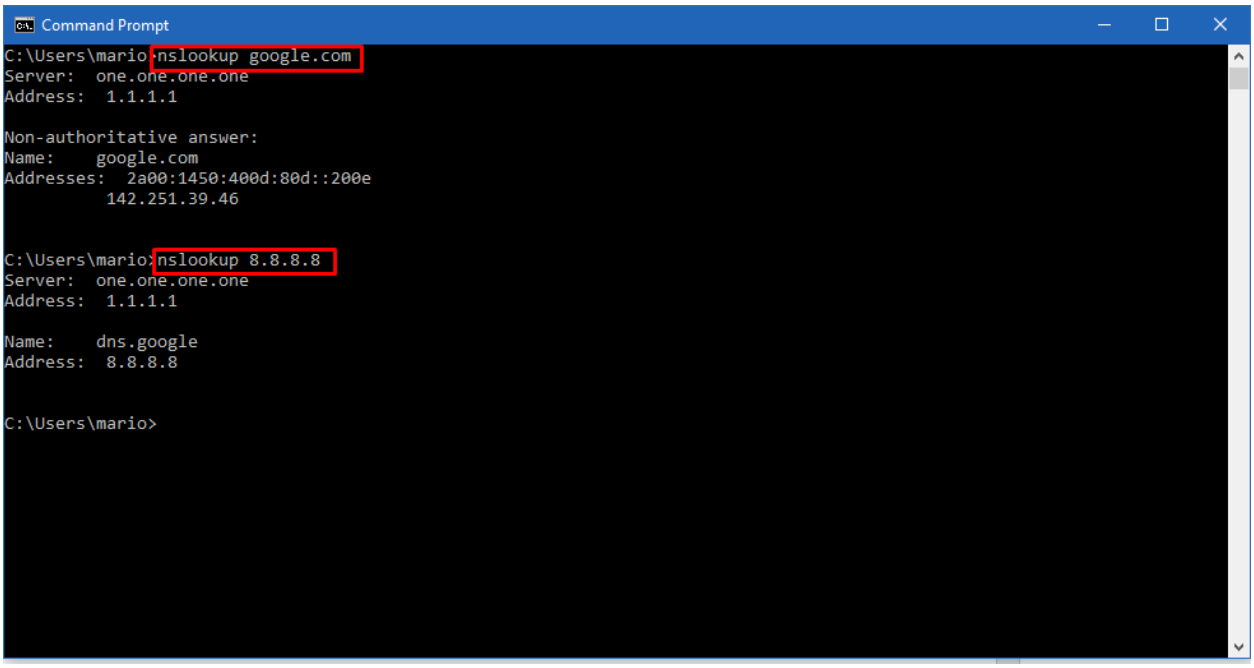
Jednostavnije rečeno, DNS služi kako bi dodijelio ime nekoj javnoj IP adresi koja je dinamička te se mijenja iz nekog DHCP bazena.

Za primjer, imamo server na kojem se nalaze neki podaci (word dokumenti, excell, pdf…), ako taj server ima javnu IP adresu (dodijeljena od strane Mrežnog providera), te nije statična nego je dinamička, moramo tom serveru dodijeliti ime koje će iza sebe uvijek imati adresu koja će u tom trenutku biti aktualna.

Tako ćemo imati javnu IP adresu 89.215.72.133 te ćemo dodijeliti tom serveru DNS ime na primjer, FileServer01 te ćemo isto to ime zapisati unutar DNS servera.

DNS isto tako služi kako bi pohranjivao poznate mu adrese u imena koja su im dodijeljena.

Google.com iza sebe ima jednu od adresa 8.8.8.8 i 1.1.1.1, ovo možemo provjeriti jednostavnom naredbom **nslookup** google.com u CMD.



Slika 1 - nslookup naredba u CMD-u

Izvor slike: Osobno računalo

VPN

Virtual Private Network je mreža odnosno vrsta protokola koja služi za povezivanje na internet drugom IP adresom odnosno maskira stvarnu IP adresu u onu koja je određena kako bi se ušlo u nečiji intranet s namjerom, pristupilo stranicama dostupnim za određene Zemlje ili pak kako bi se prekrio „identitet“ samog „hosta“ to jest, korisnika računala koji koristi ovaj protokol.
Ova vrsta mreže je vrlo bitna za daljnje razumijevanje dokumentacije jer je jedan od načina spajanja u tuđu mrežu.
Kako bismo jednostavnije shvatili ovu vrstu mreže, uzeti ćemo za primjer nešto što je u današnje vrijeme vrlo aktualno, a to je rad od kuće.
Mnoga poduzeća su odlučila svoje zaposlenike poslati raditi od kuće ako im to uvjeti dopuštaju.
Da bi ti isti zaposlenici mogli raditi od kuće, moraju nekako pristupiti podacima koji su pohranjeni na njihovim internim serverima u poduzeću.
Jedan od načina da dođu do istih je gore spomenuta mreža.
OpenVPN, Forticlient, Mikrotik VPN, TunnelBear su samo od nekih programa koji nude ovu vrstu mreže kako bi pristupili serveru koji logički nije u vašoj mreži kod kuće.
Kod kuće je vaše računalo recimo, dobilo IP adresu računala 192.168.100.88, no u Vašem poduzeću se koriste adrese u DHCP bazenu od 10.10.1.2 do 10.10.1.254
To znaći da se logički računalo iz kućne mreže i server koji ima adresu na primjer, 10.10.1.75, neće vidjeti jer nisu u istom „bazenu“ adresa a ni istoj mreži.
Da bi ta dva hosta iliti računala bila vidljiva jedno drugome, jedan od načina je da se koristi VPN servis.
VPN servis će u spajanju dodijeliti kućnom računalu adresu 10.10.1.25.
Sada je kućno računalo vidljivo serveru odnosno ono glumi kao da je fizički priključeno na mrežu u tom poduzeću.
Nakon spajanja, kućno računalo će moći pristupiti svim podacima na tom serveru kao da je u tom poduzeću.

DHCP

Dynamic Host Configuration Protocol jest protokol koji je sam po sebi u teoriji jednostavan, a uloga mu je ta da zapravo dodjeljuje IP adrese „hostovima“ koji su na mreži.

DHCP uvelike pojednostavljuje i zapravo čini mogućim da svako računalo ili mrežni uređaj ima svoju jedinstvenu IP adresu unutar nekog „bazena“ (eng. Pool)

DHCP bazen (Pool)

Ovo je dio protokola s kojim se određuje koje će se adrese koristiti za dodjeljivanje računalima i mrežnim uređajima.

Uzmimo na primjer prije spomenuto poduzeće koje je imalo u svojoj infrastrukturi DHCP bazen s adresama od 10.10.1.2 do 10.10.1.254.

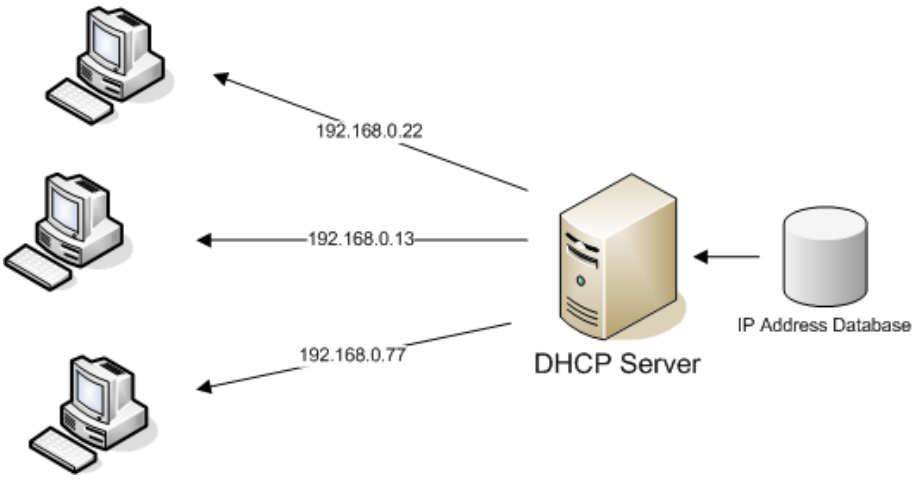
DHCP protokol će sam uzimati adrese iz ovog raspona adresa i dodjeljivati računalima

Network ID i Broadcast adresa

Kao što se može primijetiti, 10.10.1.1 i 10.10.1.255 nisu IP adrese koje su gore navedene.

Prvo spomenuta (10.10.1.1) jest Network ID adresa i služi kako bi se prepoznala mreža po kojoj teče sav internet promet do te interne mreže, često nazivana i Gateway adresa (prolaz)

Drugo spomenuta adresa (10.10.1.255) je broadcast adresa i služi za prepoznavanje i slanje podataka do svih uređaja koji moraju dobiti jednaku poruku unutar poduzeća koje koristi te IP adrese.



Slika 2 - Ilustracija dodjeljivanja IP adresa

Izvor slike: https://cybersecuritynews.co.uk/how-does-dhcp-work/

Port Forward (Otvaranje/Prosljeđivanje portova)

Još jedan od načina povezivanja na neki server ili mrežu unutar nekog intraneta ili sustava jest port forward.

Sam po sebi, služi zapravo za prepoznavanje puta na transportnom OSI sloju, kako bi se nekim IP adresama ili DNS imenima dodijelili posebni brojevi za pristup nekom od servisa ili sustava.

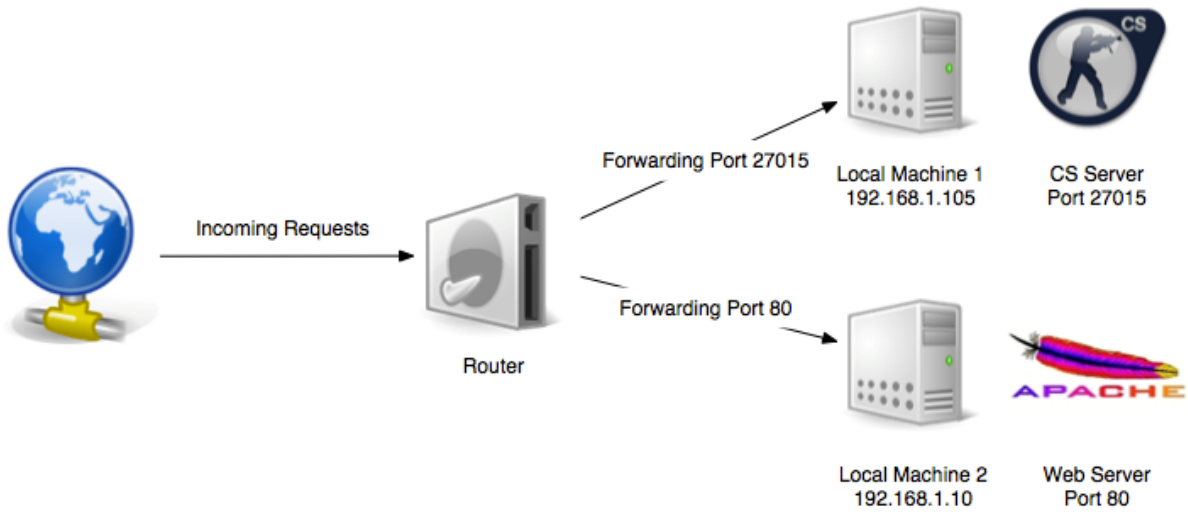
Za primjer uzmimo server koji smo prije spomenuli, **FileServer01,** u ovom slučaju, neka ima statičku IP adresu, te je na njemu neki ERP sustav na koji se moraju spajati vanjski komitenti.

Server ima adresu 10.10.1.25 ili DNS ime FileServer01, no ako ćemo to ukucati putem Http servisa ili RDP protokola, spojit ćemo se direktno na server.

Kako bismo došli do ERP sustava koji ima svoj GUI (Graphical User Interface), moramo na neki način precizirati putanju do koje će doći klijent do tog ERP sustava.

Tu dolazi Port forward s kojim se određuje poseban broj za povezivanje na sami sustav.

Nadalje ćemo detaljnije objasniti samo korištenje ove mrežne opcije.



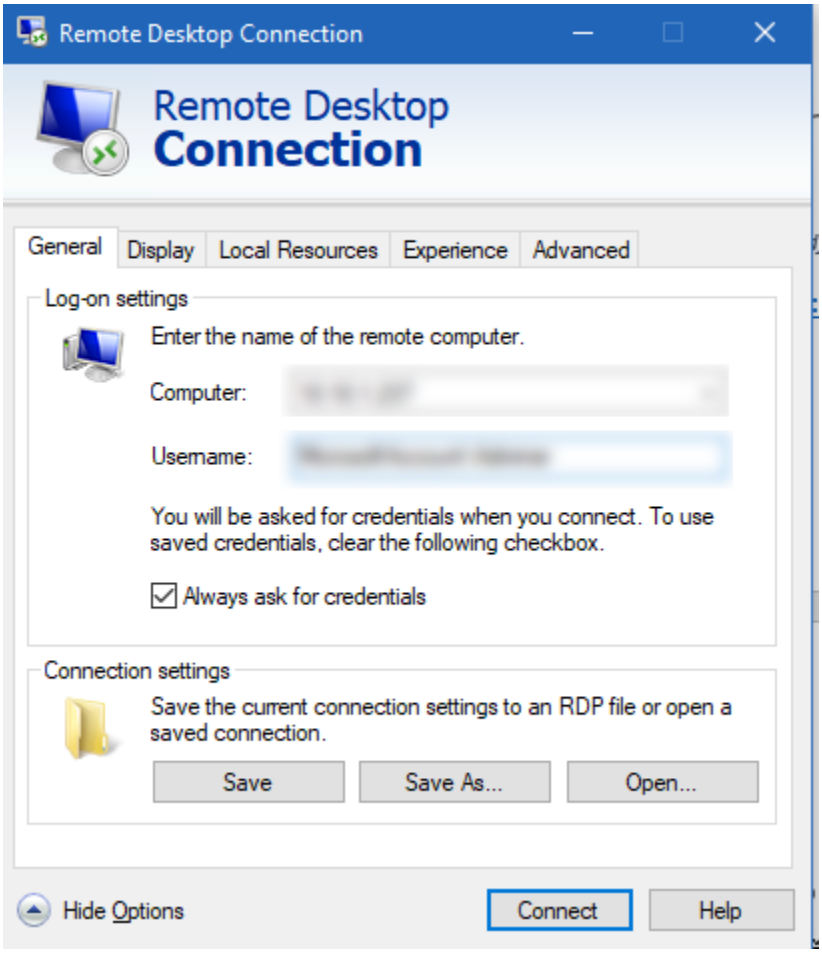
Slika 3 - Port Forward

Izvor slike: https://www.electrical4u.net/network/what-is-port-forwarding/

RDP

Remote Desktop Protocol je vrsta spajanja na neko računalo ili server putem IP adrese ili DNS imena sa korisničkim imenom i lozinkom te ako postoji, portom koji je određen za spomenuto računalo ili server.

Otvara se u obliku prozora i izgleda kao da ste na svom računalu.



Slika 4 RDP prozor

Izvor slike: osobno računalo

SFTP

Secure File Transfer Protocol je isto jedan od načina koji može poslužiti kao transfer podataka, no u ovom dijelu ćemo pojasniti na koji način funkcionira.

Za povezivanje putem ovog protokola, mora postojati server računalo i host (korisnik).

Najčešće je definiran kao vrlo siguran način prijenosa podataka putem interneta jer može koristiti više vrsta sigurnosne prijave na jedan takav sustav.

Filezilla ili WinScp su jedan od najčešće korištenih programa za ostvarivanje ovakve vrste konekcije.

Ono što ga posebno odvaja od ostalih je visoka razina sigurnosti i pouzdanost protoka podataka jer koristi najčešće TCP protokol za provjeru slanja paketa i prijenosa istih.

SFTP protokol se koristi javnom IP adresom ili DNS imenom kako bi se spojio na neki od servera i obavezno koristi portove za povezivanje na SFTP server.

Default (Uobičajeni) port za SFTP protokol je 22, no nije praksa da se koristi jer je tada i vrlo laka meta hakerima koji raznim alatima napadaju IP javne adrese i slanje podataka po tom portu te tako identificiraju koliki promet se šalje i prima preko istog.

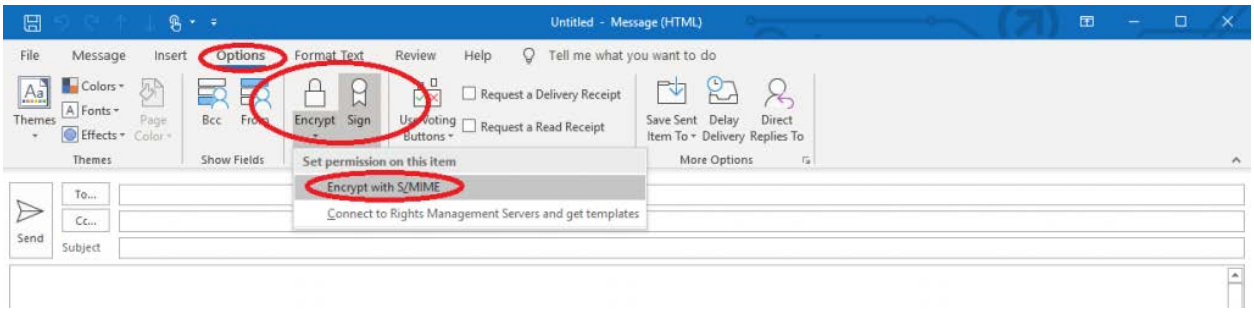
Two-Factor authentication (2FA)

Još jedan sigurnosni sloj zaštite u protokolima autentikacije koji osigurava dodatnu sigurnost iznad samog korisničkog imena i lozinka.

U posljednje vrijeme, sve više sustava, programa i stranica koristi spomenuti sloj zaštite kako bi sebi osigurali posao, odnosno, sve više firmi zbog sigurnosti uvodi ovaj način autentikacije jer jedino na taj način mogu sebi osigurati suradnju s firmama kada se radi o prijenosu povjerljivih podataka.

Prijenos podataka putem emaila

Kada se radi o prijenosu osjetljivih podataka (Isplatne liste, financijska izvješća, podaci o ekonomiji poduzeća) ovaj način prijenosa je još uvijek najčešće korišten, jer je najjednostavniji za korištenje i samo postavljanje no uvelike kaska za visokom razinom sigurnosti jer je sami mail vrlo lako presresti.



Slika 5 - S/MIME protokol

Izvor slike: Osobno računalo

Slika 5 prikazuje jedan od načina osiguravanja da email dobije samo osoba kojoj je taj mail određen.

S/MIME protokol

Vrsta protokola koja sadrži šifriranje poruke ključem koji dobije primatelj tog emaila.
Nakon što se definira primatelj putem elektroničke pošte (Njegov Email), tom email se dodjeljuje javni ključ i time se kreira vrsta tunela na način da mail jedino dobije osoba koja posjeduje isti taj ključ.
Ovaj protokol je dostupan u mnogim mail programima a jedan od njih je Outlook koji je često korišten u srednjim i većim poduzećima.

Prednosti

Brzina

Kao jedna od najvećih prednosti, možemo je opisati kao vrlo brzi način slanja povjerljivih podataka putem javnih mreža jer je potrebno par poteza u samom programu kako bi se izvršilo slanje podataka.

Učinkovitost

Slanje i primanje mailova je proces koji se događa u sekundama i vrlo je efikasan način jer koristi najniže slojeve OSI strukture odnosno koristi TCP protokol te samim time, ne postoji email koji neće doći do druge strane a da pošiljatelj nije o tome obaviješten.

Jednostavnost i dostupnost.

Mail program kao takav je vrlo jednostavan za postaviti a isto tako način slanja putem S/MIME protokola je vrlo jednostavno,

Pretplate na 0365 licence su sada već vrlo pristupačne s cijenama i dostupne skoro svima, te samim time dostupne široj publici koja se koristi elektroničkom poštom.

Mane

Sigurnost

Elektronička pošta je jednostavna za presretanje čak i uz S/MIME protokol te kao takva vrlo je nesigurna.

Isto tako, mailovi korišteni u samom programu imaju svoju cache memoriju, odnosno, i bez internetskog pristupa su dostupni korisniku i to unazad par mjeseci (Ovisno o postavkama).

Ovo naslućuje na činjenicu da kod krađe samog laptopa ili samog tvrdog diska je vrlo lako doći do podataka koji su se slali u elektroničkoj pošti.

Posrednici i manjak dokaza o presretanju

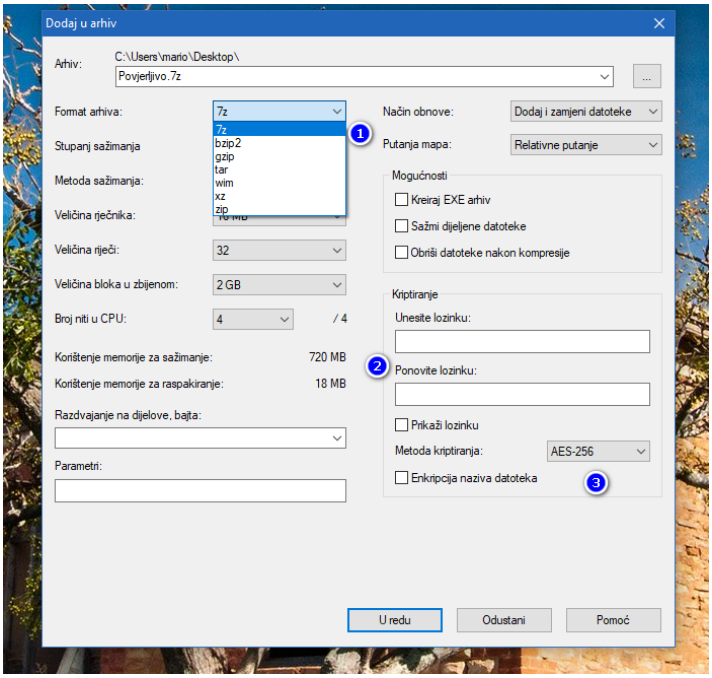
Svaka elektronička pošta negdje je spremljena, ako ne više, onda privremeno dok ne dođe do primatelja nekog podatka, ovo potencijalno može značiti da se bez dokaza može „backdoor“ metodom (Metoda da se iza nekog programa dođe do samih protokola i podataka gdje se sve sprema) doći do elektroničke pošte koja u sebi sadrži povjerljive podatke a da to nitko ne može poslije primijetiti da je ukradeno.

Potencijalna rješenja

Kako bismo povećali razinu sigurnosti slanja povjerljivih podataka putem elektroničke pošte, možemo osigurati kriptiranje same datoteke koja se šalje u elektroničkoj pošti.

7Zip

Ovaj mali program može poslužiti kako bismo zaključali odnosno kriptirali datoteku koju želimo poslati sa lozinkom koju možemo razmijeniti s primateljem elektroničke pošte putem SMS-a ili pozivom.



Slika 6 - Način kriptiranja

Izvor slike 6: Osobno računalo

Korak 1: odabiremo format same datoteke nakon arhiviranja

Korak 2: Upisujemo lozinku koju želimo da se koristi za otključavanje same datoteke

Korak 3: Metoda kriptiranja (Ovdje postoji više vrsta koje definiraju kompleksnost same lozinke)

Winrar

Program sličan prije spomenutom 7Zipu no ima malo drukčiji izgled i to je zapravo glavna razlika ako pričamo o kriptiranju podataka. Više se koristi jer je stariji i više publike je čulo za Winrar nego za 7Zip.

Prijenos podataka putem direktnih kanala na server pomoću VPN protokola

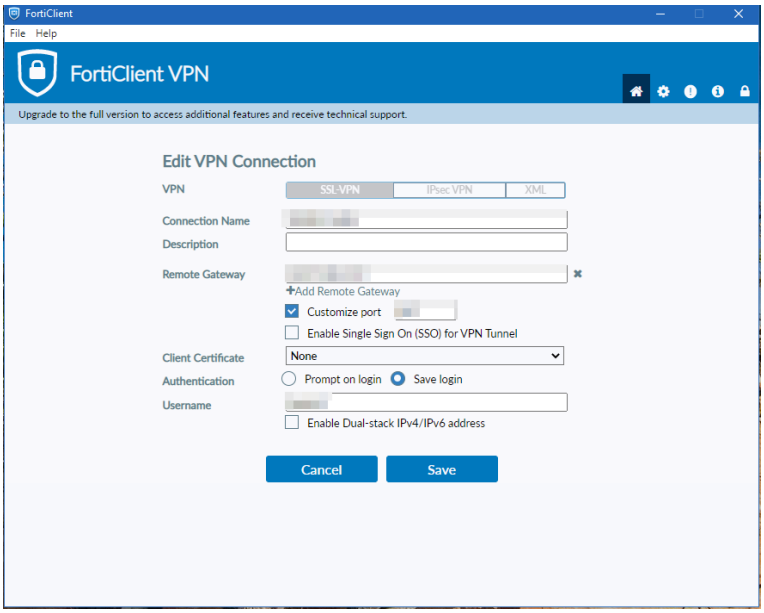
Ova vrsta prijenosa podataka je nešto manje korištena globalno gledajući no sve više prihvaćena zbog trenutne situacije u svijetu koja je većinu uredskih poslova preselila u domove zaposlenika.

Ova vrsta prijenosa podataka iziskuje znanje za postavljanje takve vrste povezivanja i napredniju infrastrukturu u samom poduzeću.

Kao jedan od osnovnih uvjeta za kreiranje ovakve vrste podataka je program koji podržava VPN protokol. Nadovezat ćemo se na FortiNet VPN Client kao ogledni primjer.

Sami program nije dovoljan naravno, uz njega još moramo imati:

Usmjerivač (Router), Server na kojem su podaci i internet vezu.



Slika 7 - FortiClient VPN sučelje programa

Izvor slike: Osobno računalo

Slika 7 prikazuje kako izgleda program za spajanje na mrežu poduzeća.

U ovom programu se definira ime servera odnosno adresa usmjerivača (Ili ip adresa Gateway usmjerivača) do koje se mora korisnik spojiti kako bi pristupio serveru na koji mora spremiti podatke i datoteke.

Nakon samog spajanja na mrežu od poduzeća, korisnik je dobio IP adresu iz DHCP bazena jednakog kao da je u samom poduzeću gdje je server na koji se šalju podaci i datoteke.

Samim time, dobio je pristup svim datotekama na serveru i omogućeno mu je slanje podataka direktno na sami server u pripadajuće datoteke.

Prednosti

Učinkovitost

Naravno, kad pričamo o prednostima kod VPN protokola, učinkovitost je ovdje na visokoj razini jer je VPN u današnje vrijeme vrlo stabilna veza i osigurava prijenos podataka s vidljivim tragom i lakoćom pronalaska tko je i kad nešto preuzeo ili poslao na sami server.

Sigurnost

Vrlo velik broj (Pa tako i FortiClient VPN) podržava 2FA metodu duple autentikacije spajanja, što znači da nije dovoljno posjedovati korisničko ime (Username) i lozinku (Password) već i jednokratnu lozinku ili neku vrstu odobrenja s treće strane kako bi povezivanje na vanjsku mrežu bilo uspješno. Neki od načina su pomoću Microsoft Authenticator aplikacije koja se spaja pomoću Active Directory korisničkog računa i samog usmjerivača kako bih u vrijeme spajanja na vanjsku mrežu, poslala na telefonski broj mobitela (Najčešće, može i samo da izbaci odobrenje spajanja) jednokratnu lozinku koja se mora upisati na program koji se koristi za VPN protokol.

Trag slanja/primanja podataka je lako dostupan

Ovo je vrlo važna stavka kod samog prijenosa podataka i povjerljivih datoteka, jer recimo, da dođe do zlonamjernog korištenja samih podataka, uz pomoć korisničkog imena koje se koristilo tokom slanja/primanja, vidi se točno tko i kad je koristio koje podatke te samim time na temelju korisničkog imena, možemo utvrditi tko je koristio račun za potencijalnu krađu podataka.

Mane

Cijena

Da bismo osigurali ovakav način spajanja, potrebno je imati vlastitu infrastrukturu.

Usmjerivač, file server, internet provider, licenca za VPN program (Najčešće po korisniku) su jedne od najskupljih stavki kod ovakvih infrastruktura koje mogu doseći cijene od par desetaka tisuća eura.

Naravno, ako je u interesu poduzeća da su podaci sigurni i da ne dođu u krive ruke, onda cijena nije bitan faktor, no svakako je stavka koja uvelike utječe na odluku o načinu razmjene povjerljivih podataka.

Potrebne vještine i znanje za postavljanje ove vrste razmjene podataka

Kako bi se VPN protokol i spajanje na file server odradio da funkcionira kako treba i po standardu, potrebna je visoka razina znanja kako u mrežnom, tako i sistemskom dijelu informatike

Mreža

Potrebno je znanje postavljanja VLANa (Virtual Local Area Network) za dobivanje IP adrese iz posebnog DHCP bazena iz usmjerivača.

Postavke na samom usmjerivaču što se tiče DNS zapisa

Sistemska strana

Kreiranje korisničkih profila na Active Directoryu

Povezivanje Active Directorya i korisničkih profila kreiranih na samom VPN programu s licencama

Davanje prava po korisniku kako bi se odredila hijerarhija po datotekama.

Stabilna i brza internet veza

Mnogi VPN programi imaju minimalne uvjete za internet vezu, odnosno, provjeravaju Bandwith same veze na mreži koju klijent koristi.

To znači da na primjer, neki VPN program neće raditi ako će latency (vrijeme potrebno da paket bitova dođe s mjesta A na mjesto B) biti veći od 30 ms (30 milisekundi za slanje jednog paketa/bita), download brzina biti manja od 25 mbps te upload brzina manja od 10 mbps.

Potencijalno velik problem, jer u HR mnoga mjesta ne ispunjavaju te uvjete kod providera.

Kada se koristi ovaj način spajanja do povjerljivih podataka i slanja istih ?

Kada pričamo o sigurnosti, ovo je daleko bolji način razmjene povjerljivih podataka nego putem elektroničke pošte, no isto tako, ovaj način spajanja traži i relativno kompliciranu edukaciju za korisnike kako i na koji način funkcionira ovakva vrsta spajanja i razmjene podataka.

Kada se počne pričati o VPN, 2FA, port forwardu, čak i korisnici koji imaju neku vrstu informatičkog znanja, mogli bi se zbuniti u ovim pojmovima.

No, ako želimo sigurnost i učinkovitost, ovo je način razmjene podataka koja je jedno od rješenja.

Naravno, VPN omogućava potpuno spajanje u mrežu nekog poduzeća ili tuđe mreže, što omogućuje da se spaja na sve mrežne uređaje u toj mreži, pa tako i na printere, druge server i ostale servise kao na primjer, ticketing sustav, web aplikacije i ostalo.

VPN nas ne ograničava samo na korištenje File Servera i prijenosa datoteka, nego na daje pregršt opcija kao da smo fizički u poduzeću.

Kada se ulazi u ovakav projekt, moramo uzeti u obzir da se ovakav način razmjene podataka koristi kada se većina komitenata i zaposlenika spaja na udaljenu intranet mrežu koja im nije fizički dostupna.

Kada bi imali 90% komitenata i zaposlenika fizički u poduzeću, tada ovaj način razmjene nema nikakvu svrhu i resursi ne bi bilo korisno uloženi.

Vjerojatno i najvažniji razlog ovog načina spajanja je situacija u kojoj se trenutno cijeli svijet nalazi i potencijalno kako će rad izgledati u budućnosti a to je rad od kuće.

Situacija a i neke europske prakse su pokazale da rad od kuće je itekako povoljna i dobrodošla stvar, kako za zaposlenika, tako i za poslodavca.

Vjerujem da će načelno rad od kuće kao takav, natjerati mnoga poduzeća i tvrtke da ulažu u baš ovaj načina spajanja jer im je dostupna cijela infrastruktura poduzeća ili tvrtke kao da su fizički tamo.

Zaključak o ovom načinu spajanja

VPN protokoli u današnje vrijeme su sve sigurniji i stabilniji što se tiče samog rada s istima. Pružaju velike mogućnosti u smislu same konfiguracije postavki, delegiranja prava za svakog zaposlenika odnosno korisnika koji će se spajati s ovim načinom.

Sve su popularniji zbog same situacije u svijetu gdje većina ljudi radi od kuće pa se koristi ovim načinom spajanja u svoje poduzeće i ima pristup svim podacima uz minimalan napor i informatičko znanje.

Rekao bih čak da od svih prije navedenih protokola, ovaj zasad drži vodeće mjesto u smislu „dobiveno-uloženo“ s obzirom na sve mane koje ima i ako uzmemo u obzir da si jedno poduzeće može priuštiti ovakav jedan informacijski sustav koji sam po sebi nudi visoku razinu sigurnosti, pouzdanost i fleksibilnost rada i održavanja sustava.

No, moram spomenuti još jednu vrlo važnu stavku u ovoj priči, a to je zlouporaba ovog protokola.

Spajanje putem VPN-a (ovisno o pružatelju protokola/programa i postavkama) može u potpunosti zamaskirati IP adresu s koje koristite mrežu, to jest, izlazite van na internet s adresom koja može biti predstavljena kao da ste u nekoj drugoj državi ili na nekom drugom računalo.

Ovo jednom laiku ne znači ništa, no zamislite da „rudarite“ kripto valute i prenosite na jedan račun to sve, i pritom, koristite IP adresu od poduzeća jer, naravno, brzina u jednom srednjem do velikom poduzeću je ogromna, (1 Gigabit ili 10 Gigabit) i može pružiti mnogo veće pogodnosti za neke, da kažemo, nedopuštene radnje.

Jedna od njih je i preuzimanje licenciranih proizvoda koji su „piratizirani“ s torrent stranica. Preprodaja, korištenje te distribucija takvih proizvoda koji su preuzeti s ilegalnih stranica je protuzakonita a kada maskirate svoju mrežu s mrežom od svog poduzeća, tada izgleda onima koji to prate, da se takvi podaci preuzimaju iz poduzeća, što je kazneno djelo i poduzeće može odgovarati za takve procedure i snositi velike troškove i kazne.

Prijenos podataka putem nekih od cloud usluga

Došli smo i do posljednjeg načina prijenosa povjerljivih podataka koji je svim novijim generacijama dobro poznat.

No, u amaterske svrhe ili profesionalne, ovaj način prijenosa i pohrane podataka je vrlo diskutabilan te se mnogi stručnjaci i zakoni lome oko toga da li uz sve dodatne mjere sigurnosti, je ovaj način distribucije podataka siguran i pouzdan kako to sve tvrtke koje pružaju ovaj način pohrane, tvrde.

U nastavku ću se dotaknuti nekih od najpoznatijih cloud pružatelja usluga i navesti glavne karakteristike od svakoga kako bismo na kraju imali jasnu sliku o čemu se ovdje zapravo radi.

Citrix ShareFile

Citrix kao takav nam je svima poznat jer je sestrinska firma od Cisco koja je poznata po svojim moćnim i skupocjenim mrežnim uređajima korištenima svugdje po svijetu.

U besplatnoj verziji cloud računa, nudi isprobavanje same usluge pohrane podataka na njihov oblak, a početna cijena je nekih 50 $ za 5 zaposlenika u poduzeću.

U tom se paketu odmah nudi i integracija s njihovim DUO Mobile aplikativnim rješenjem za 2FA.

Vrline

Ovaj pružatelj cloud usluga je vrlo profesionalan, ima na internetu vrlo visoke ocjene korisnika, vrlo pouzdan i radi besprijekorno.

Čak i u start/basic paketu nudi neograničen cloud prostor i integraciju 2FA spajanje što je za današnje standarde vrlo bitno zbog sigurnosti rada s razmjenom podataka.

Mane

Ako govorimo o masovnom korištenju ovog programa, recimo za 300+ zaposlenika, ova vrsta usluge može itekako povećati mjesečne troškove jednog poduzeća.

Najskuplji paket za velika poduzeća doseže cijenu od otprilike 330 $ što je itekako mnogo.

Najgore je to što neka poduzeća i firme ne žele prihvatiti prijenos podataka putem oblaka te morate uz ovo rješenje, imati i druge usluge dostupne za klijente.

DropBox Business

Malo više poznat amaterskoj publici, odnosno ljudima koji ne koriste toliko sve dosad navedene usluge, ovaj pružatelj je više nastrojen manjim poduzećima i mnogo više ga koriste ljudi koji imaju u vlasništvu Apple proizvode jer je od početka bio baziran na apple uređajima pa zbog toga, savršeno radi i na Mac računalima.

Kao takav, radit će najnormalnije i na mobilnim uređajima i pružat dokumente i sadržaj kao da ste na svom računalu.

Prednosti

Standard verzija odnosno početna verzija kod ovog pružatelja iznosi svega 12 $ mjesečno za 5 korisnika s 3 TB prostora.

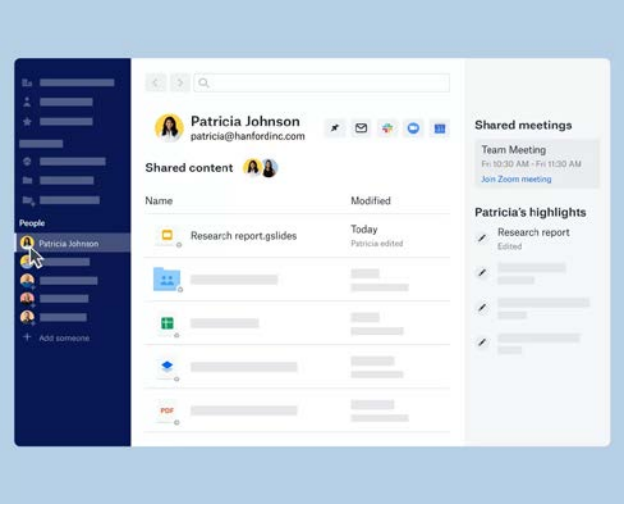
Nudi individualno zaključavanje podataka lozinkom.

Samo Web sučelje je vrlo jednostavno a nudi i program za desktop računala.

Mane

Pati od manjka dodatne 2FA sigurnosti koja je danas neophodna za profesionalan prijenos podataka.

Vrlo često se nađe u kritikama profesionalaca kao pružatelj s neprofesionalnim pristupom kada se radi o prijenosu podataka što je djelomično točno jer sami cloud pružatelj nudi zaključavanje AES-256 protokolom individualno zaključavanje podataka.



Slika 8 - DropBox Business

Izvor slike: https://www.webimp.com.sg/business/dropbox-business-vs-personal/

Microsoft SharePoint

Možda ne spada u punom smislu pod cloud poslužitelja, ali sama baza i srce ove platforme jest pohrana te samim time ulazi u ovu skupinu, a i nalazi se u oblaku.

Mnogima možda manje poznata, pogotovo ako se nikad nisu susretali s Office 365 sustavom, ova platforma je zapravo najsigurnija, najtočnija, najveća i najprofesionalnija od svih prije navedenih.

Microsoft SharePoint je predstavljen još davne 2001. godine no tada je bio namijenjen samo za pohranu podataka i dokumenata.

Nakon toga se razvio i pretvorio u platformu za spremanje web stranica i kreiranje istih, no to nije dugo trajalo i pretvorio se u potpunosti u Cloud based platformu za pohranu koja sada služi u Office 365 sustavu potpunu integraciju svih podataka kroz tu platformu.

To znači, da ako na primjer, neko poduzeće koristi Office 365 full paket, znači teams, office programe, One drive, Active Directory, Azure Systems, svi podaci ikad spremljeni kroz navedene sustave se mogu pronaći na SharePointu.

Prednosti

Pošto je sam sustav integriran i spojen kao jedno, nudi sve sigurnosne protokole koji osiguravaju minimalne uvjete za neke od najstrožih ISO certifikata na svijetu.

2FA ima integriranu i sa DUO mobile aplikacijom i s MFA (Multi Factor Authenticator by Microsoft)

Dostupan je i putem weba i putem desktop aplikacije.

Vrlo je brz i nema nikakvih sigurnosnih propusta u zadnjih desetak godina.

Mane

Cijena kao takva ne može biti definira zato jer Sharepoint dolazi isključivo uz Office 365 platformu za server pa samim time i mnogo košta, a to znači i po par tisuća dolara mjesečno za velika poduzeća.

Manjak znanja za delegiranje prava po korisnicima može stvarati napor za informatičare koji održavaju jedan ovakav sustav jer iziskuje visoku razinu informatičarskog znanja.

Kada koristiti razmjenu podataka putem cloud pružatelja usluga ?

Kao što sam već na početku rekao, ovaj način razmjene podataka, pogotovo s povjerljivim tipom je vrlo diskutabilan.

Mnoga poduzeća i klijenti neće pristati na razmjenu podataka ovim načinom jer, iako nude sigurnost i 2FA koji je jedan od uvjeta za ISO 27001, boje se kako ne bi došlo do curenja podataka s one treće strane, a to je sam pružatelj usluge.

Morate biti svjesni da kod svakog sličnog prijenosa podataka uvijek postoji posrednik, a ovdje je to pružatelj usluga, jer, ipak, svi ti podaci jesu na oblaku, no ustvari, to je negdje pohranjeno fizički na nekom file serveru i uz nekoliko grešaka, te informacije i podaci između Vas i klijenta, mogu vrlo lako „procuriti“

Zato će zapravo svako ozbiljnije poduzeće izbjegavati ovaj način za prijenos podataka o plaćama, financijskim izvješćima poduzeća, stanjima na računima i slično jer ne mogu klijentima garantirati sigurnost i povjerenje jer ovise o trećoj strani.

Neka poduzeća koja ne prenose podatke najviše sigurnosti će odabrati ovaj način za razmjenu podataka jer ne moraju svojim klijentima garantirati da će podaci uz tuđu grešku dospjeti u krive ruke.

S druge strane, vrlo je praktičan način jer ne iziskuje nikakvu dodatnu opremu ili serverska rješenja kako bi se podaci pohranili nekud i tako podijelili s drugom stranom.

Naravno, možemo i sami stvoriti „cloud“ pohranu, to jest, kreiramo jedan file server, napravimo aplikativno rješenje, dizajniramo aplikaciju i desktop program i tako pristupamo svojim podacima i delegiramo tko može do tih podataka a tko ne, no onda zapravo opet imamo prije spomenutu situaciju sa samim serverom u našem poduzeću, osim ako ćemo imati server na udaljenoj lokaciji, onda bi to bila druga priča, no tad bi se odmaknuli od same ideje pružatelja takvih usluga jer bi sami sebi bili pružatelj usluga a to nam nije bio cilj u ovoj opciji.

ISO 27001

Mnogo puta ovdje spomenut, no što je zapravo taj poznati certifikat kojeg je zapravo vrlo teško za dobiti no vrlo lako za izgubiti ?

U daljnjem tekstu će biti objašnjeno što je točno taj certifikat.

„ISO 27001 je međunarodni standard objavljen od strane Međunarodne Organizacije za Standardizacije (ISO) i opisuje kako upravljati informacijskom sigurnošću u tvrtkama. Najnovija inačica ovog standarda je objavljena 2013. godine, te je sadašnji puni naziv ISO/IEC 27001:2013. Prva revizija standarda je objavljena 2005. godine a razvijena je na temelju britanskog standarda BS 7799-2.

ISO 27001 može biti implementiran u bilo kojoj organizaciji, profitnoj ili neprofitnoj, privatnoj ili državnoj, maloj ili velikoj. Napisali su ga najbolji svjetski stručnjaci na polju informacijske sigurnosti i propisuje metodologiju za primjenu upravljanja informacijskom sigurnošću u organizaciji. Također, omogućava tvrtkama dobivanje certifikata, što znači da neovisno certifikacijsko tijelo daje potvrdu da je organizacija implementirala informacijsku sigurnost sukladno ISO 27001.

ISO 27001 je postao najpopularniji standard informacijske sigurnosti u svijetu, te su mnoge kompanije certificirane prema njemu – ovdje možete vidjeti broj certifikata u posljednje dvije godine.

ISO 27001 je usredotočen na zaštitu povjerljivosti, cjelovitosti i raspoloživosti podataka u tvrtki. To se postiže prepoznavanjem koji se potencijalni problemi mogu dogoditi podacima (tj. procjena rizika), te definiranje što treba poduzeti da se takvi problemi spriječe (tj. tretman ili obrada rizika).

Sigurnosne mjere koje će se implementirati su obično u formi politika, procedura i tehničke primjene (npr. softvera i opreme). Međutim, u većini slučajeva tvrtke već imaju sav potreban hardver i softver ali ih koriste na nesiguran način – stoga se većina primjene ISO 27001 odnosi na uspostavu organizacijskih propisa (tj. pisanje dokumenata) koji su neophodni da bi se spriječilo narušavanje sigurnosti.“

Izvor teksta: https://advisera.com/27001academy/hr/sto-je-iso-27001/

A što je s digitalnim potpisima i zlouporabom istih te kako se nečiji potpis može ukrasti i zloupotrijebiti ?

Kako i svi ostali navedeni protokoli su izloženi zlouporabi, tako ni ovaj ne oskudijeva od ostalih.
Naime, digitalni potpisi su relativno stara tehnologija, no nije se koristila unatrag nekoliko godina dok nije postala sigurnija i fluidnija u radu.
Adobe Acrobat je nudio ovakvu vrstu potpisa na dokument ali samo u svojoj plaćenoj verziji te je ovakav način tada bio u početku znatno skuplji.
No, s vremenom, maknuli su plaćanje ove opcije odnosno ubacili su digitalni potpisu u besplatnu verziju adobe pdf čitaća.
Funkcionira na način da se potpis kao takav fizički skenira, pospremi se u obliku digitalnog formata i doslovno spremi na jedan od USB uređaja za potpisivanje dokumenata s certifikatom osobe čiji je potpis.
Slično kao internet bankarstvo, trebate USB uređaj s certifikatom koji ste dobili iz FINE, programsku podršku da bi mogla učitati takvu vrstu datoteka i program za digitalno potpisivanje dokumenata za neke firme.
Jedina razlika je u tome što kod osobnog digitalnog potpisa, ne možete ovjeravati neke dokumente ako nemaju još i poseban certifikat za specifične dokumente.
Konkretno, možete staviti potpis na neki dokument sa svojim digitalnim potpisom, ali ne možete i „potpisati“ dokument odnosno ovjeriti ga za neku firmu za daljnju obradu.
Zvuči kompliciranо, no ustvari radi na vrlo jednostavan način.
Mnoga poduzeća su počela koristiti digitalno potpisivanje jer olakšava rad s klijentima koji su fizički udaljeni i ne mogu uvijek u neko izvjesno vrijeme nešto potpisati a hitno je.
No svaka korisna i relativno jednostavna metoda načina odrade nekog posla donosi sa sobom i neke negativne strane za one čiji potpis vrijedi mnogo i može se iskoristiti za kojekakve zle namjere i kaznena djela.
U nastavku ću raspodijeliti kao i prije prednosti i mane ovog načina „razmjene“ podataka jer kada bolje sagledamo ovakav protokol, on je itekako neka vrsta razmjene podataka i informacija jer s jednim bitnim potpisom mogu se razmijeniti svakakvi podaci i informacije.

Prednosti

Iako u ne tako davnoj prošlosti, digitalno potpisivanje se trebalo platiti na način kupnje adobe acrobat paketa za takvu vrstu procesuiranja podataka.

No, kako je tehnologija išla naprijed, tako je i Adobe maknuo samo plaćanje i uveo da ta opcija bude u potpunosti besplatna.

Jedino što se treba platiti jest taj USB uređaj i FINA certifikat koji imaju relativno nisku cijenu.

Jednostavnost je jedna od osobina ovog načina procesuiranja podataka.

Sve što trebate znati jest par pritisaka na samom programu, staviti potpis na željeno mjesto na skenirani dokument i to je to, Vaš je dokument potpisan kao da ga je odgovorna osoba potpisala na licu mjesta.

Brzina je isto tako još jedan od pojmova koji se mogu usko vezati za digitalno potpisivanje. Program kao takav radi besprijekorno, još ako imate adekvatno računalo i internet brzinu, potpisivanje i dijeljenje dokumenta je završeno u tren oka.

Autentičnost kao takva se može vezati s ovim potpisivanjem na način da svaki put kad stavite potpis, dobijete i digitalni datum kad je potpis stavljen i broj autorizacije tako da uvijek možete provjeriti vjerodostojnost samog potpisa.

Mane

Kao i svaki prijašnji način autorizacije i prijenosa podataka, i ovaj ima neke loše strane i rupe koje se mogu zlouporabiti.

Prvi i najštetniji je sama zlouporaba potpisa.

Dali ste USB uređaj s vašim potpisom novom zaposleniku, on je odlučio napraviti totalni kaos u poduzeću i potpisao je gomilu dokumenata na štetu Vašeg poduzeća.

Manjak tehničkih sredstava se može protumačiti u smislu da morate nešto potpisati a prestao je raditi Vaš dobri stari laptop. U ovakvim situacijama ćete se uvijek sjetiti dobrog starog papira i olovke gdje se rijetko kad moglo desiti da baš u tom trenutku nema nikoga oko Vas da vam posudi kemijsku olovku na par sekundi da potpišete ugovor, a ako vam ne radi laptop a u kafiću ste, teško ćete naići na nekoga tko će Vam samo tako posuditi svoj laptop

Da li koristiti digitalno potpisivanje ili ipak ne ?

Nekad Vas situacija natjera da morate koristiti sredstva koja nisu u Vašoj domeni ili jednostavno niste ugodni s korištenjem istih, no nemate izbora i sila Vas natjera na korištenje.
Digitalno potpisivanje se tek uvodi u svijet računovodstva i srodnih djelatnosti, nije da se ne koristi, no manja poduzeća i dalje prakticiraju dobar stari način s kemijskom olovkom i papirom.
Treba biti objektivan i sagledati stvari s više kutova.
Pristalica sam digitalnog potpisivanja jer vjerujem da se mora ići u korak s vremenom jer tehnologija toliko brzo napreduje da se možete pronaći u situaciji da Vaši resursi i tehnologija koju Vaše poduzeće koristi više nije u upotrebi a onda ste u veliki problemima.
Naravno da nije uvjet da neko poduzeće funkcionira normalno ili ne ako imate ili nemate digitalno potpisivanje, no uz minimalan trud da naučite kako isti koristiti i primijeniti u svom poduzeću je mala cijena za ono što dobivate a to je štednja vremena sebi da čekate nadležnu osobu da potpiše taj dokument i osobu čiji je potpis jer sigurno ima i drugih bitnijih poslova od samog potpisivanja jedne stranice ugovora a svi znam da je vrijeme novac.
Sve prije navedene metode razmjene podataka kao i ova su dugo poznate informatičkom svijetu no tek u zadnjih nekoliko godina dolaze do izražaja zbog svih situacija u svijetu i digitalizacije oko nas.
Bolest koja hara, napredak računala i informatičkih sustava dovodi i najveće laike informatike da uče i nadograđuju svoje znanje kako bi mogli koristiti tu tehnologiju u svom poduzeću.
Mnoga poduzeća su se tako u zadnjih 3 godine prebacila na potpuni rad od kuće i primjenjuju sve protokole za razmjenu podataka koje sam ovdje naveo.
Samim time, jedan računovođa se tako susreće i sa VPN programom, spajanjem na mrežu poduzeća, slanje mailova kriptiranim putem, korištenje cloud usluga pa i digitalno potpisivanje mu prođe kroz ruke koji put.
Svakako bi se digitalno potpisivanje trebalo globalizirati još više i postati primijećeno u srednjim i velikim poduzećima jer bi se na veću količinu ljudi uštedilo mnogo vremena koje se može iskoristiti za korisnije stvari

Zaključak

Cilj i poanta ovog rada je bila elaborirati i pojasniti samo razmjenu povjerljivih podataka između dva poduzeća ili klijenta i poslužitelja.

Naveo sam glavne i jedine kandidate za razmjenu podataka koji mogu ispuniti minimalne tehničke uvjete i zadovoljiti neke svjetske norme što se tiče sigurnosti i razmjene povjerljivih podataka.

S gledišta profesionalizma i najviše moguće razine sigurnosti, mogu sa sigurnošću reći da je Prijenos podataka putem direktnih kanala na server pomoću VPN protokola najbolji mogući izbor što se tiče trenutne tehnologije koja se nudi u svijetu informatike.

Svako poduzeće će pristati na korištenje takvog sustava za prijenos podataka jer podliježe svim sigurnosnim protokolima i ispunjava sve uvjete za najbitnije certifikate koje neka firma može tražiti od Vas da bi surađivala i dijelila podatke s Vama i Vašim poduzećem.

Naravno, svako korištenje, brisanje, nadopunjavanje i ostale radnje na dokumentima su vidljive i može im se ući u trag te isto tako se mogu kreirati i dnevna ili mjesečna izvješća tko je i kad koristio koje podatke na nekom serveru.

Isto tako, točno se utvrđuje tko delegira prava za djelatnike i kome su dana prava za koje podatke.

Ako se i mijenjaju ljudi s potpunim pravima na te dokumente, isto tako podliježu zakonu da ako zlouporabe dokumente, biti će pravovaljano sankcionirani, a ne mogu pobjeći od toga, jer kao što je prije spomenuto, za svaki postupak na tim dokumentima postoji trag.

Kritičko prosuđivanje mog odabira za idealnog kandidata za prijenos podataka jest to da sve ima mane i prednosti, no kod više odabira i mogućnosti, moramo gledati što nam je prijeko potrebno, za što imamo sredstava i što je tehnički moguće u našem poduzeću.

Sve to kada se skupi u jednu cjelinu, dobijemo rezultat da ako radimo s dokumentima visoke razine povjerljivosti, moramo uložiti u siguran rad s istima i pouzdane kanale prijenosa istih, kako bismo klijentima omogućili nesmetan rad i garantirali svojim protokolima i informacijskim sustavima da će njihovi podaci biti sigurni 24 sata na dan, 31 dan u mjesecu i 365 dana u godini te da za svaki gubitak podataka ili informacija, imati ćemo trag i dokaze tko i kada je zlouporabio dokumente i u koje svrhe.

Izjava o autorstvu završnog rada i akademskoj čestitosti

Ime i prezime studenta: Mario Kujundžić

Matični broj studenta: 6-010/19-ITI

Naslov rada: Razmjena povjerljivih podataka putem interneta sigurnosnim protokolima i način spajanja s interneta na intranet

Pod punom odgovornošću potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada.

Potvrđujem da je elektronička verzija rada identična onoj tiskanoj te da je to verzija rada koju je odobrio mentor.

Datum	Potpis studenta
18.3.2022.	Mario Kujundžić 

Internetski izvori

https://advisera.com/27001academy/hr/sto-je-iso-27001/

https://www.webimp.com.sg/business/dropbox-business-vs-personal/

https://www.electrical4u.net/network/what-is-port-forwarding/

https://cybersecuritynews.co.uk/how-does-dhcp-work/

Popis slika

Mario Kujundžić

Date of birth: 17/09/1993 | **Nationality:** Croatian | **Gender:** Male |

(+385) 995186517 | mariokujundzic993@gmail.com |

Pustodol 94 c, 49240, Donja Stubica, Croatia

WORK EXPERIENCE

20/05/2012 – 29/10/2018

TEHNICIAN – GIGATRON RAČUNALA

-maintenance of computers
-setting up cash registers
-setting up network servers
-RDP costumer support
-repairing windows,desk setups
-soldering circuit boards
-Setting up Windows and Mac OS
-Maintenance of security camera systems
-Printer and fax setups
-Registry editor repairs

Oroslavje, Croatia

21/03/2019 – 24/05/2019

WAITER – CRYSTAL SYMPHONY CRUISES

-Taking care of dishes
-Serving food and beverages to guests
-setting up tables

01/09/2019 – 01/05/2021

ICT NETWORK TECHNICIAN – CALLIDUS GRUPA D.O.O

-Servers maintenance and set up (setting up RAID,UPS monitoring systems,patching RJ45 and Rj11,Lansweeper monitoring and creating new reports,Veeam off site backup creating,mremoteNG rdp management,creating virtual machines based on WIN OS and Linux)
-Websites maintenance in cPanel.
-MS Access management and configuring for smaller bussines
-Hardware soldering and repairing notebooks.
-Wifi4EU project,(configuring APs and Antennas,going on terrain and setting up on locations for hotspots),making schemes for towns in MS Visio.
-SonicWall Portforwarding,all-in-one systems set up,making new VPN connections for inner or outter hosts.
-Active directory using on daily base (adding new users,enabling and disabling new drive paths for power users and regular users,droping in specific groups)
-Exchange outlook; creating users and mointoring cloud space
-cPanel mail system and website maintenance
-mRemoteNG servers managment for DC controllers,AD Server,DHCP servers,DNS servers
-Adding new users in active directory,making new hosts in DNS servers for IP resolving,controlling IP's in DHCP.

-Exchange service (creating distribution groups,delegations,exceptions for mailboxes,expanding mailbox storage,domain control maintenance.
-Office 365 cloud support for office licenses , windows key activations and management of client accounts.
-Support for all-in-on office package, full management.
-HTML and CSS basic knowledge
-SQL basic knowledge
-Winbox mikrotik routers set up and conf.
-Making new VPN connections for hosts,L2TP and SSTP with PSK.
-Setting up VPN connections through Windows built-in or Netextender or GVC.
-Veeam Backup management, Sonicwall creating VPN users, blacklist hosts creating, whitelist creating.
-DNS Hosts importing

Zagreb, Croatia

01/05/2021 – CURRENT – Zagreb, Croatia
SYSTEM ENGINEER – DATA LINK UNIJA IT

Full helpdek maintenance of 98 people in company
Migration of servers and network equipment
Full backup and restore with Veeam Backup utility
Full O365 Maintenance (Exchange security, creating new OU, Creating security rules and exceptions for Exchange server, Teams utility admin center)
Synology backup NAS drive, setting up virtual VLAN's for backup network
Full Active Directory management
Creating OU inside AD
Fortinet and mikrotik routers network management level 2 (Maintenance, creating VLANS)
Creating RAID Fields level 2 (Creating RAID 1,0,5 and 6)
ESXI installation and creating new Virtual desktops
VMWARE host center backup and maintenance
Support for all smaller problems (Teams, skype, RDP, Net banking, network issues)
Full hardware support (CPU removal, upgrade, thermal paste replacing, GPU replacing, diagnostics, upgrading)
Creating Seminars and educational videos for co-workers
Tutotorials and how-to videos for understanding of new technology used in our company (Such as using new remote support app, using new VPN program and how to connect to internal network and etc.
Responsible for taking care of our domains and expanding their date of expire
Full Office 365 maintenance plan considering Active directory sync with domain controller
Teams integration of one drive for business file share inside company
Sharepoint maintenance
Exchange compliant and security flow
Full backup of .pst files through ediscovery creating protocol
Fortinet firewall setup and maintenance
Migration of server room and full stack network restore
Leading team of people for migrating 80+ people from one location to another in terms of network and IT equipment

EDUCATION AND TRAINING

01/09/2008 – 21/05/2012 – Oroslavje, Croatia
COMPUTER TEHNICIAN – Srednja škola Oroslavje

English Language (speaking,writing,listening on high level)
CNC preparing and input mapping
Desk setup maintenance
Lan network setup
soldering circuit boards

10/10/2019 – CURRENT – Zaprešić, Croatia
VELEUČILIŠTE BALTAZAR – Information Technology (IT)

English
SQL
HTML & CSS
Microsoft Servers
OOP

LANGUAGE SKILLS

Mother tongue(s): **CROATIAN**

Other language(s):

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken production	Spoken interaction	

- **COMMUNICATION AND INTERPERSONAL SKILLS**

Extrovert at its highest level

-Very friendly, can overcome any situation related to people that i dont know and having communication problems.
-Can adopt to any kind of new situation in every society
-Multicultural-friendly with experience working with multiple cultures at once
-Highly adoptive to new situations, locations and new job sites.
-Adventure type of person, loves to travel, connects with other poeple and meet new technology aswell as making new friends.
-Very communicative and have excellent contact skills gained through my experience as waiter with children and older population as well.
-Can entertain guests/co-workers and make them smile and comfortable in my surrounding

-Want to learn in near future at least 2 languages (Spanish and French)
-Ready to promote any kind of events as well as new
assortments and educational seminars by myself

This is my link to my LinkedIn Profile so you can check it out :)
linkedin.com/in/mario-kujundžić-9a22b4196

- **JOB-RELATED SKILLS**

Job-related skills

-Network maintenance
-Administrator
-Web design maintenance
-Backup full utility management
-Creating RAID fields
-Restoring and creating ESXI machines; virtual or Hardware and etc.

01/01/2019 – CURRENT

Half-Time support for small-business companies

taking care of personal computers
Ethical hacking and reverse engineering on guest and internal network
Antivirus solution integration
Setting up office package and windows installation
Full maintenance of network equipment remotely or off-site