Bekim Dauti

Siguria e Rrjeteve Kompjuterike

Teknikat dhe Teknologjitë

Siguria e Rrjeteve Kompjuterike:

Teknikat dhe Teknologjitë

nga Bekim Dauti

Ky e-Libër i dedikohet të gjithë lexuesve të cilët bëjnë hapat e parë ose tashmë i kanë bërë ato në fushën e sigurisë së rrjeteve kompjuterike. Krahas informimit dhe ndarjes së diturisë, qëllimi i këtij e-Libri është që të kontribuoj në ngritjen e njohurive profesionale në shoqërinë tonë. Kështu, largojmë paditurinë dhe ngritemi në nivelet e shoqërive të civilizuara teknologjikisht. Zot na e shto diturinë.

Faleminderit Zotit që më dhuroi jetë, shëndet dhe mundësi që sado pak të jap kontributin tim në ndarjen e diturisë. Zoti e shpërbleftë familjen time, miqtë, kolegët dhe të gjithë që më përkrahën në përpilimin e këtij e-Libri.

Përmbatja

Hyrje

I dashur lexues, qëllimi i këtij e-Libri është që të ju paraqes hyrjen në sigurinë e sistemeve kompjuterike përmes teknikave dhe teknologjive të sigurisë së rrjeteve kompjuterike. Duke pas parasysh faktin se ditë e më shumë në Internet lexojmë raporte për shkelje të intimitetit dhe thyerje të sigurisë të sistemeve kompjuterike, andaj uroj që ky e-Libër sado pak të luan rolin e informatorit për rëndësinë e sigurisë qoftë individuale deri sa lundrojmë në Internet apo të sistemeve dhe rrjeteve kompjuterike të bizneseve.

Për nga numri i faqeve e-Libri është i shkurtë! Por kjo nuk do të thotë se nuk arrin të përmbush qëllimin e tij. Pra, ideja ka qenë që e-Libri të jetë konciz dhe të përmbajë informata të rëndësishme për teknikat dhe teknologjitë e sigurisë së rrjeteve kompjuterike.

Si lexues i librit, ju jeni komentuesi dhe kritiku më i rëndësishëm. Me këtë, çmoj mendimin tuaj dhe dëshiroj të dijë:

- vlerësimin tuaj për këtë e-Libër?,
- si mund ta bëjë më të mirë këtë e-Libër?, si dhe
- çfarë risi teknologjike të sigurisë së rrjeteve kompjuterike dëshironi të përmbajë ky e-Libër?

andaj, gjeni pak kohë për të dërguar një e-Postë të shpejtë deri tek BekimDauti@BekimDauti.com, ashtu që së bashku me ju ta përmirësojmë këtë e-Libër akoma.

Kapitulli 1: Çka është siguria?

Kur marrim vendimin për të vendosur siguri në një mjedis të caktuar pune, gjëja e parë që do të bëjmë është të vlerësojmë kërcënuesit potencial të një mjedisi të tillë pune. E njëjta gjë vlen edhe për sigurinë e rrjeteve kompjuterike! Përmes identifikimit të kërcënuesve të mundshëm të rrjetit kompjuterik, ne rrisim shanset që të zgjedhim zgjidhjen më të mirë të mundshme për siguri të rrjetit kompjuterik. Ne përgjithësi, kur duam të merremi me ndonjë çështje në mënyrë të duhur, atëherë rekomandohet qe të posedojmë njohuritë adekuate dhe përvojën në atë lëmi. Në mënyrë të njëjtë, në rastin e vendosjes së sigurisë në rrjete kompjuterike duhet të dimë se çfarë është siguria e rrjeteve kompjuterike dhe si implementohet ajo? Sipas fjalorit Webster, siguria në përgjithësi definohet si "*gjendje ose cilësi e të ndjehurit i lirë nga frika, shqetësimi ose përkujdesi*". Kështu, definicioni për rrjetin e sigurt për komunikim është "*rrjeti, përdoruesit e të cilit nuk ndjejnë frikë apo shqetësim përderisa përdorin shërbimet në të*".

Në ditët e sotme, vërejmë numër të madh të teknologjive të përdorura nga bizneset për të siguruar rrjetet e tyre kompjuterike. Por shtrohet pyetja: vallë kërcënimi për shërbimet ne rrjete kompjuterike vjen gjithmonë nga jashtë apo ka diçka me shumë se kaq? Raportet flasin që përveç sulmeve të organizuara qe vijnë nga jashtë perimetrit të rrjetit kompjuterik të organizatës, më shumë se gjysma e tyre vijnë nga brendia e perimetrit të rrjetit, në veçanti nga nëpunësit. Shpesh dëgjojmë se si nëpunësi pa dashje ka shkelur sigurinë e ndërmarrjes se tij ose rastet kur ndonjë e metë ne aplikacionet softuerike ka shkaktuar ndaljen e disa shërbimeve ne rrjet apo edhe mosfunksionimin e tërësishëm të rrjetës. Kjo bënë që përgjegjësit dhe sistemet e tyre të sigurisë duhet të jenë më vigjilent si ndaj sulmeve nga jashtë e po ashtu edhe ndaj atyre nga brenda.

Në kapitujt në vijim do të shpalosim disa nga teknikat dhe teknologjitë e disponueshme në ditët e sotme për të siguruar intimitetin individual si dhe shërbimet në rrjetet kompjuterike të bizneseve.

Kapitulli 2: Zhvillimet e reja në teknologjinë e informatikës

"Bëhu bujar. Kjo është këshilla e parë dhe e fundit për të gjithë ata që duan të jenë të dobishëm dhe të lumtur në dobitë e tyre." Charles W. Eliot

Askush nga ne nuk e vë në dyshim dobinë që marrim nga kompjuteri, aq më tepër nga një kompjuter i lidhur në Internet! Porse e keni pyetur vetën se çfarë duhet të jetë një kompjuter që t'i jetësojë këto dobi në vlerën (pothuajse) 100%? Përpiquni ta gjeni përgjigjen e kësaj pyetje nga këndi i sigurisë në fushën e teknologjisë së informatikës. Pajtohem që kompjuteri nuk është një risi në shkencën e teknologjisë së informatikës, po aq sa edhe ju pajtoheni që ka qenë dikur një i tillë. Duke pas në konsideratë faktin që të gjithë kërcënuesit kanë për synim një qëllim siç është ai i cenimit të dobive që gjeneron kompjuteri, atëherë mund të konkludojm që sot për të jetësuar dobitë nga puna me kompjuter nevojitët më shumë se posedimi i një hardueri të një prodhuesi të njohur, më shumë se një sistem operativ i licencuar, më shume se një antivirus, më shumë se një antispyware, më shumë se… Thjeshtë, po aq sa teknikisht është i avancuar kompjuteri juaj, kërkohet që edhe përdoruesi i tij të posedojë njohuritë e duhura!

Është mirë të dihet për CERT!

CERT është qendra për ekspertizë të sigurisë së Internetit me vendndodhje në Institutin për Inxhinieri Softuerike, një qendër për hulumtim dhe zhvillim e përkrahur nga fondet federale dhe e drejtuar nga Universiteti Carnegie Mellon në Pittsburgh, Pennsylvania. Objektivë studimi i kësaj qendre janë lëshimet në sigurinë e Internetit, hulumtimet e ndryshimeve afatgjatë të sistemeve të rrjetëzuara, si dhe zhvillimi i informatave dhe trajnimeve për t'u ndihmuar përdoruesve të skajshëm dhe organizatave me qëllim të përmirësimit të sigurisë. Në vitin 1988, kur krimbi Morris ndërpreu 10% të sistemeve të Internetit Agjensioni për Hulumtime në Projektet e Avancuara të Mbrojtjes (DARPA) angazhoi SEI që të themelon një qendër e cila do të ketë për detyrë të koordinon komunikimin në mes të ekspertëve në situata emergjentë të sigurisë dhe të ndihmon në evitimin e incidenteve në të ardhmen. Kjo qendër u quajt CERT Coordination Center (Cert/CC).

Përderisa vazhdon të përgjigjet në incidentet madhore të sigurisë dhe të analizon lëshimet në produkte, roli i saj është zgjeruar përgjatë viteve. Së bashku me rritjen e hovshme të madhësisë së Internetit dhe përdorimit të tij për funksione kritike, ka pasur ndryshime progresive në teknikat e ndërhyrjeve, rritje të sasisë së dëmeve, rritja e vështirësive në detektimin e sulmeve dhe natyrisht rritje e vështirësive në kapjen e sulmuesve. Me qëllim të menaxhimit sa më të mirë të këtyre ndryshimeve CERT/CC tashmë është pjesë e një programi më të madh objektivat primare e të cilit janë të sigurojë se po përdoren praktikat e duhura për menaxhim të teknologjive dhe sistemeve ashtu që t'u rezistojnë sulmeve në sistemet e rrjetëzuara dhe kështu të kufizojnë dëmin dhe të garantojnë vazhdimësinë e shërbimeve kritike pavarësisht sulmeve të suksesshëm, aksidenteve apo edhe dështimeve. Disa nga lëmit e punës së CERT/CC janë: analiza e lëshimeve dhe incidenteve të sigurisë, menaxhimi i mbijetesës së shërbimeve në korporata, edukimi dhe trajnimi, inxhinieria e mbijetesës së sistemeve dhe aktivitete tjera të rëndësishme.

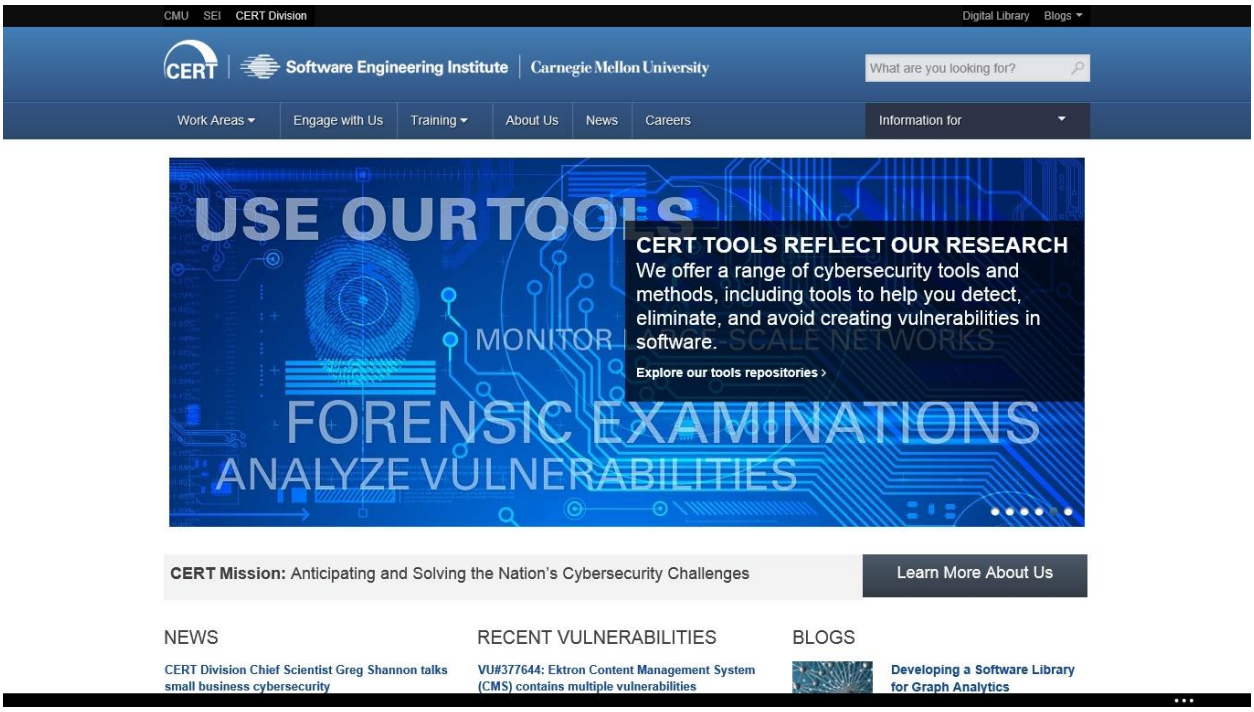


Figura 1. Ueb faqja e CERT® Coordination Center

Misioni i CERT/CC

CERT/CC është i privilegjuar të punoj me komunitetin e Internetit në detektimin dhe zgjidhjen e incidenteve të sigurisë kompjuterike, gjithashtu edhe në ndërmarrjen e hapave konkret për parandalimin e incidenteve në të ardhmen. Në veçanti, misioni i tyre është të:

- Ofrojë një pikë të vetme kontakti të besueshëm, të sigurt dhe 24 orësh për situata emergjentë,
- Ndihmojë në komunikimin në mes të ekspertëve që punojnë në zgjidhjen e problemeve të sigurisë,
- Shërbejë si pikë qendrore për identifikim dhe korrigjimin e lëshimeve në sistemet kompjuterike,
- Mirëmbajë lidhje të ngushta me aktivitetet hulumtuese dhe të bëjë hulumtime në përmirësimin e sigurisë në sistemet ekzistuese dhe
- Ndërmarr masa proaktive për ngritjen e vetëdijes dhe të kuptuarit të sigurisë së informacionit dhe të çështjeve të sigurisë së kompjuterëve në mesin e komunitetit të rrjetit të përdoruesve dhe të ofruesve të shërbimeve.

Si ta kontaktoni CERT/CC?

Po që se klikoni në lidhjen Contact në ueb faqen www.cert.org, do të vëreni opsionet në vijim për ta kontaktuar CERT/CC. Ato janë:

- **e-Posta:** po që se dëshironi të raportoni lëshimet në softuerin për rrjetë me anë të postës elektronike mund ta përdorni Formularin për Raportimin e Lëshimeve.
- **Shifrimi i të dhënave të ndjeshme:** duke qenë se ju po dërgoni të dhëna të ndjeshme përmes postës elektronike gjë që kjo nuk është e rekomanduar, atëherë rekomandoheni që ti shifroni ato me anë të Pregty Good Privacy (PGP) teknologjisë për shifrim të të dhënave.
- **Linja direkte telefonike:** edhe përkundër orarit të punës nga ora 08:00h e deri në 17:00h, sërish në situatat e raportimit tuaj përmes telefonit dikush do të përgjigjet edhe jashtë orarit përfshi këtu fundjavat dhe festat.
- **Faks:** ekziston edhe kjo mundësi e raportimit.

- **Adresa postare:** nëse e parapëlqeni raportimin përmes metodave tradicionale të komunikimit, atëherë thjeshtë vendoseni raportin tuaj në zarfe dhe sigurohuni që keni shënuar adresën postare të CERT/CC.
- **Marrëdhëniet publike:** natyrisht që ekziston edhe ky opsion i komunikimit me CERT/CC.

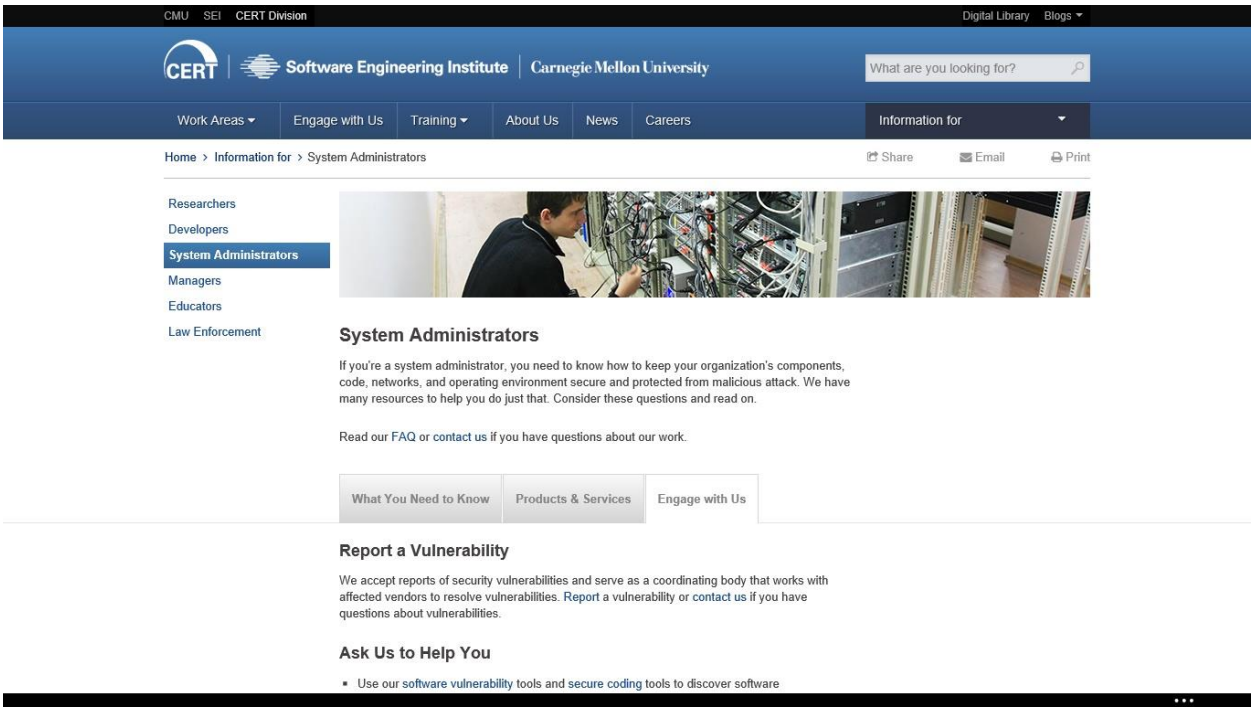


Figura 2. Si ta kontaktoni CERT/CC?

Konkluzioni: Përse CERT Coordination Center?

Që të ngritët vetëdijesimi për çështjet e sigurisë dhe të ndihmohen organizatat të përmirësojnë sigurinë e sistemeve të tyre, CERT/CC mbledh dhe shpërndanë informatat nëpërmjet kanaleve të shumta. CERT/CC liston resurset që mund të jenë të nevojshëm për t'u ballafaquar me viruset. Gjithashtu, CERT/CC publikon dokumente me temat nga më të ndryshmet të sigurisë. Indeksi i publikimeve të tyre ofron lidhjet deri tek artikujt, raportet teknike dhe të hulumtimit si dhe punimeve shkencore të publikuara nga stafi i tij. Së bashku me US-CERT, CERT/CC publikon paralajmërimet për problemet e sigurisë së Internetit. CERT/CC posedon mundësinë që të punojë së bashku me të tjerët në përmirësimin e sigurisë së Internetit dhe të mbijetesës së rrjetit. Dhe më e rëndësishmja nga të gjitha, është fakti që CERT

Coordination Center është aktive në organizatat e shumta të cilat janë të përkushtuara në sigurimin e sistemeve të informatikës.

Kapitulli 3: Kriptografia në një vend!

"Jeta është ndryshim. Zhvillimi është opsional. Zgjedh me mençuri." Karen Kaiser Clark

Kriptografia ka ekzistuar qe kur ekziston njerëzimi! Që kur njerëzimi filloi të komunikoj, u paraqit nevoja e fshehjes së komunikimit. Përgjatë historisë, kriptografia është konsideruar me shumë si art se sa një disiplinë shkencore. Edhe pse teknikat matematikorë luajnë rol të rëndësishëm ne kriptografi, serish ajo nuk bazohet vetëm në funksionet matematikore. Sot, kriptografia është bërë një teknikë e zakonshme e komunikimit në mes të individëve, grupeve, organizatave dhe korporatave, sidomos për faktin që komunikimi i informatës është bërë më i rëndësishëm dhe më me vlerë se kurdo herë më parë.

Historia e kriptografisë

Kriptografia thuhet të jetë një nga fushat më të vjetra të hulumtimeve teknike për të cilën mund të gjenden gjurmë nga historia njerëzore deri në 4000 vite më parë. Ishin hieroglifët që dekoronin varret e sundimtarëve dhe mbretërve. Këto shkrime me hieroglifë tregonin historitë jetësore të mbretërve duke shpalosur edhe veprimet fisnike të tyre. Kinezët e lashtë përdornin natyrën ideografike të gjuhës së tyre për të fshehur domethënien e fjalëve. Mesazhet zakonisht transformoheshin në ideografe për qëllime intimiteti. Për dallim nga Egjipti dhe Kina, në Indi shkrimet sekretë ishin dukshëm më të avancuara, përfshi këtu edhe pushtetet e kohërave të tilla të cilët përdornin kodet e fshehura për të komunikuar me spiunët e shpërndarë nëpër gjithë vendin. Historia e kriptografisë të Mesopotamisë ishte e ngjashme me atë të Egjiptit, ashtu që shkrimi kuneiform përdorej për të shifruar tekstin. Në dramën e famshme Greke "Iliada", kriptografia është përdorur në rastin kur Bellerophon është dërguar tek mbreti me një pllakë sekretë e cila po i kërkonte mbretit ta dënojë atë me vdekje. Spartanët përdornin një sistëm të përbërë nga një fletë e hollë e papirusit e mbështjellur rreth një shtize (sot quhet "shifrues prej shtize"). Një metodë tjetër e kriptografisë qe zhvilluar nga Polybius (tashmë quhet "katrori i Polybius"). Jul Cezari përdortë sistemin kriptografik (i quajtur "Shifruesi i Cezarit") i cili zhvendos dy shkronja më tej nëpër tërë alfabetin. Arabët ishin të parët që bënë përparim të dallueshëm në fushën e kriptoanalizës. Kështu, Qalqashandi zhvilloi një teknikë për zbulimin e enkriptimit i cili përdoret edhe në ditët e sotme.

Në mesjetë, kriptografia nisi të përparoj! Më 1452, në Venedik u themelua një organizatë qëllimi i vetëm i së cilës ishte hulumtimi në fushën e kriptografisë. Leon Batista Alberti njihet si "babai i kriptografisë perëndimore", veçanërisht për zhvillimin e zëvendësimit poli alfabetik. Një hap tjetër i rëndësishëm u bë më 1518 nga Trithemius, një murg gjerman i cili shfaqi interesim të madh në okult. Më 1553, Giovan Batista Belaso zgjeroi këtë teknikë duke zgjedhur një fjalë kyçe që shkruhej mbi tekstin e dukshëm e që përdorej zakonisht për korrespondencat me letra. Më 1628, francezi Antoine Rossignol ndihmoi ushtrinë e tij të mundtë Huguenots duke bërë dekriptimin e mesazheve të kapura. Babai i kriptologjisë amerikane është James Lovell. Më 1795, Thomas Jefferson shpiku "rrotën për enkriptim". Më 1817, koloneli Decius Wadsworth zhvilloi një pajisje që përbëhej nga dy disqe, njëri brenda tjetrit ku disku i jashtëm përmbante 26 shkronjat e alfabetit dhe numrat 2 deri në 8, ndërsa disku i brendshëm përmbante vetëm 26 shkronjat. Shpikja e telegrafit me 1884, bëri që kriptografia të ndryshoj dukshëm. Kështu, më 1854 u shpik sistemi "Playfair" nga Charles Wheatstone dhe Lyon Playfair dhe qe sistemi i parë që përdortë çiftët prej simboleve për enkriptim. Më 1859, Pliny Earle Chase zhvilloi atë që njihej si shifrues i copëtuar ose tomograf. Më 1863, Kasiski zhvilloi metodën e kriptoanalizës e cila deshifronte pothuajse të gjitha enkriptimet e asaj kohe. Ashtu siç telegrafi ndikoi ne zhvillimet e kriptografisë, po ashtu zbulimi i radios më 1895 ndryshon kahun e zhvillimit të kriptografisë. Më 1917, në Amerikë formohet organizata kriptografike MI-8 me drejtor Herbert Osborne Yardley.

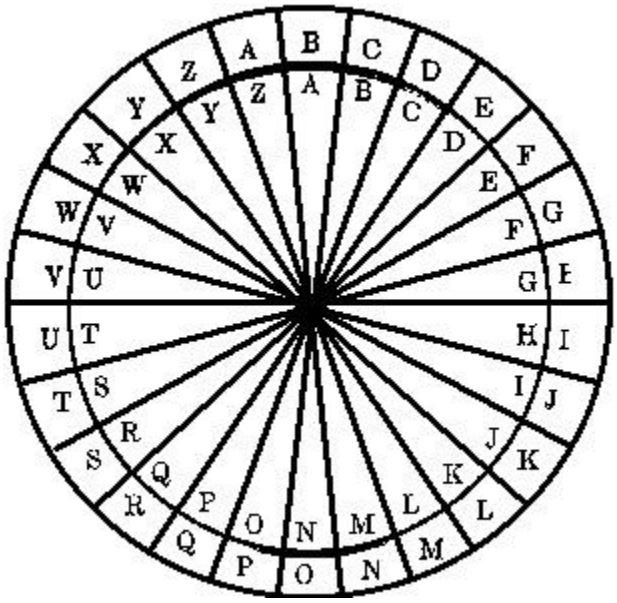


Figura 1. Shifruesi poli alfabetik (Enchanted Mind, 2002)

Përdorimi i makinave kriptografike në mënyrë dramatike ndryshoi natyrën e kriptografisë dhe të kriptoanalizës. Përparim të dukshëm në kriptografinë elektromekanike bëri zbulimi i rotorit. Gjatë luftës së dytë botërore, Suedia në cilësinë e vendit neutral pati një nga departamentet më efektive të kriptoanalizës në botë. Më 1948, Shannon publikon "Teoria e Komunikimit të Sistemeve për Fshehje". Tregimi për kriptografinë do mbaronte po të mos paraqitej nevoja praktike për dërgimin e mesazheve sekretë, në të cilat raste kërkohet që një sasi e përafërt e çelësave sekret të dërgohen paraprakisht.

Hyrje në Kriptosisteme

Sot, ekzistojnë disa terme të cilat lidhen për kriptosistemet. Këtu përfshihen kriptologjia, kriptografia, kriptoanaliza, dhe steganografia. Kriptologjia është fusha e studimit të komunikimeve të sigurta, e cila përfshinë kriptografinë, kriptoanalizës dhe steganografinë. Kriptografia është degë e kriptologjisë e cila merret me dizajnimin e algoritmeve për enkriptim dhe dekriptim. Këto algoritme kanë për qëllim fshehjen dhe autentikimin e mesazheve dhe të dhënave. Kriptoanaliza, gjithashtu, është degë e kriptologjisë që merret me thyerjen e kodeve me qëllim të rikthimit të informatës. Kodimi është një algoritëm që përdoret për enkriptim dhe dekriptim. Kodimi zëvendëson një pjesë të informatës me një objekt tjetër me qëllim të fshehjes së domethënies. Në fund fare, steganografia është metodë e kriptologjisë e cila e fshehë ekzistencën e mesazhit.

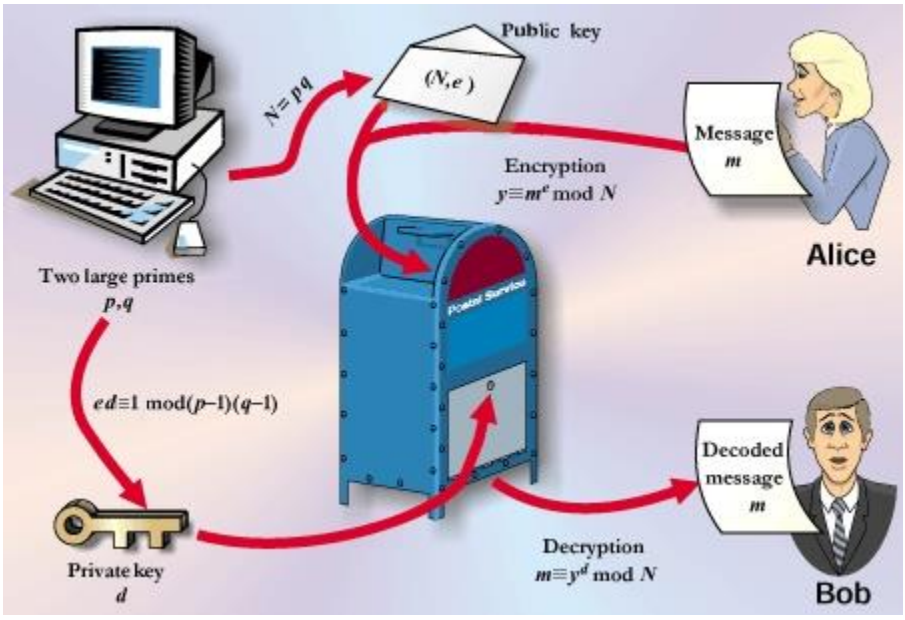


Figura 2. Principi i punës së kriptosistemet (Security Software Zone, 2007-2009)

Çka është Kriptografia?

Fjala “kriptografi” ka prejardhje nga gjuha Greke (κρυπτογραφία) që në përkthim do të thotë “shkrim sekret”. Para paraqitjes së komunikimeve digjitale, kriptografia përdorej kryesisht nga ushtria për qëllime spiunazhi. Me avancimet e bëra në komunikimet moderne, kriptologjia u mundëson bizneseve dhe individëve ta bartin informatën në mënyrë të sigurt dhe me kosto shumë të ulët përmes Internetit. Në këtë mënyrë, kriptologji ndihmon që mesazhet të bëhen të pakuptueshëm për të gjithë përveç pranuesit të mesazhit.

```
S = E
H = T
E = W
L = M
A = X

ETW EWMME EWXETWMME
SHE SELLS SEASHELLS
```

Figura 3. Një shembull kriptografik (SQL ServerCentral, 2002-2009)

Enkriptimi është një proces i cili të dhënën me përmbajtje të dukshme e transformon në të dhënë të koduar, përmbajtja e së cilës do të jetë e pamundur të lexohet pa posedimin e “çelësit”. Dekriptimi, një proces i kundërt nga enkriptimi, mundëson restaurimin e përmbajtjes së dukshme të të dhënës nga e dhëna e koduar përmes përdorimit të çelësit. Zakonisht çelësi duhet të jetë informatë sekretë dhe niveli i intimitetit të informatës së koduar varet nga fuqia kriptografike e vetë çelësit.

Kriptografia tradicionale

Kriptografia merr në shqyrtim studimin e sistemeve matematike të cilat përfshijnë dy çështje të sigurisë: intimitetin dhe autentikimin. Sistemi i intimitetit parandalon ekstraktimin e informatës nga palët e paautorizuara nga mesazhet që bartën përmes linjave publike për komunikim, duke garantuar kështu dërguesin e mesazhit se përmbajtjen e tij do ta lexon vetëm pranuesi i tij. Sistemi i autentikimit parandalon injektimin e paautorizuar të mesazheve në linjën publike për komunikim, duke i siguruar kështu pranuesit të mesazhit legjitimitetin e dërguesit të tij.

Një linjë e komunikimit thuhet të jetë publike në qoftë se siguria e saj është e pamjaftueshme për përdoruesit e saj. Kështu, linja komunikimit siç është telefoni mund të konsiderohet privatë për disa dhe publike për disa të tjerë. Varësisht nga përdorimi i saj, secila linjë për komunikim mund të preket nga përgjimi ose injektimi, apo edhe të dyjat. Në komunikimet telefonike, kërcënimi nga injektimi është shumë i lartë, meqë pala e thirrur nuk mund të përcaktojë se cili telefon po thërret. Në anën tjetër, përgjimi nga aspekti teknik është më i vështirë për tu realizuar dhe i penalizuar nga me ligj. Në komunikimet me radio, situata është e kundërt. Përgjimi është pasiv dhe nuk penalizohet nga ligji, përderisa injektimi i vë në dukje transmetuesin jo legjitim që penalizohet me ligj.

Llojet e Kriptografisë

Ekzistojnë tre lloje të formave të kriptografisë:

1. **Kriptografia me çelës të fshehur** përdorë vetëm një çelës. Me anë të këtij çelësi, mesazhi i dhënë në formë të lexueshme do të enkriptohet në mesazh të pakuptueshëm me gjatësi të përafërt sa edhe ai i lexueshëm. Në rastin e dekriptimit, përdoret i njëjti çelës që është përdorur për enkriptim. Nganjëherë, kriptografia me çelës të fshehur quhet edhe kriptografi tradicionale apo simetrike. Kodi Captain Midnight dhe MonoAlphabetic paraqesin dy lloje të algoritmeve të çelësit të fshehur, edhe pse tashmë për të dytë ekzistojnë dëshmi se thyhen lehtë. Shembuj të kriptografisë me çelës të fshehur janë: DES, Triple DES apo 3DES, International Data Encryption Algorithm (IDEA) dhe AES.
2. **Kriptografia me çelës publik** apo kriptografia asimetrike, është një disiplinë e re e shpikur më 1975. Për dallim nga kriptografia me çelës të fshehur, në kriptografinë me çelës publik çelësat nuk ndahen. Këtu, secili individ ka dy çelësa: çelësi privat që nuk duhet ti zbulohet askujt dhe çelësi publik që preferohet të jetë i ditur për secilin. Dallim tjetër i kriptografisë me çelës publik është edhe mundësia e gjenerimit të nënshkrimit digjital në mesazh. Nënshkrimi digjital është një numër i lidhur për mesazhin, që gjenerohet vetëm nga individi që posedon çelësin privat. Shembuj të kriptografisë me çelës publik janë: RSA, DSS, ElGamal, Diffie-Hellman, Zero Knowledge Proof Systems, Pretty Good Privacy (PGP) dhe Elliptic Curve Cryptography (ECC).

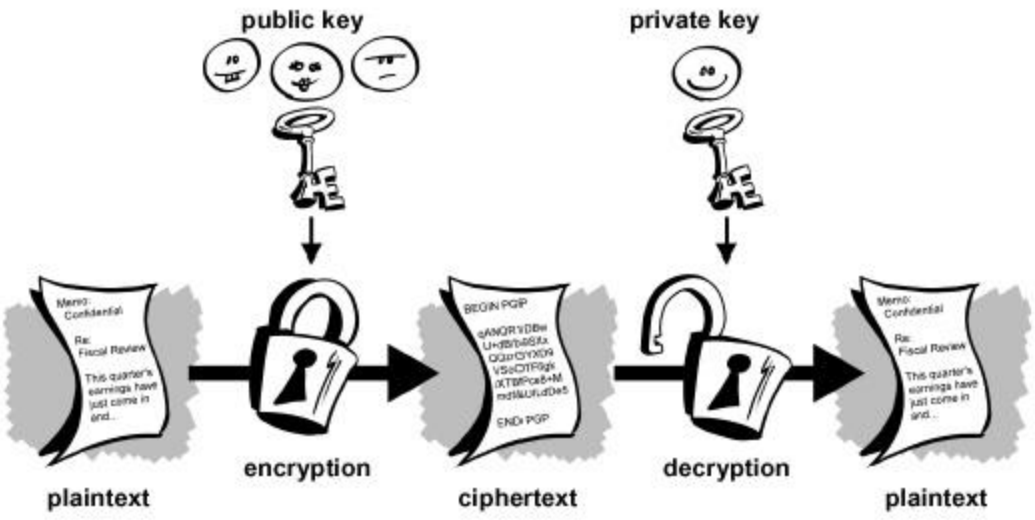


Figura 4. Kriptografia me çelës publik (http://www.akadia.com/services/email_security.html)

3. **Algoritmet hash** ndryshe njihen edhe si përvetësuesit e mesazhit ose transformuesit me një drejtim. Funksioni kriptografik hash është një transformim matematik i mesazhit me gjatësi arbitrare në një gjatësi bitësh nga e cila do të njehsohet numri me gjatësi fikse. Algoritmet hash nuk përdorin çelësat për veprimet e tyre. Shembuj të algoritmeve hash janë: Secure Hash Algorithm – 1 (SHA – 1) dhe Message Digest (MD2, MD4 dhe MD5).

Kriptografia në aksion

Ekzistojnë mënyra të shumta për ta mbajtur postën tuaj elektronike të sigurt. Një nga protokollet më të përdorura është Secure/Multipurpose Internet Mail Extensions (S/MIME), i cili është një karakteristikë e RSA-së dhe zgjerim i standardit MIME për të mbrojtur postën elektronike nga kapja, falsifikimi dhe lexuesit e padëshiruar. Duke qenë se S/MIME përdor algoritmin me çelës publik RSA, atëherë përdoruesit mund të këmbejnë çelësat edhe sikur ata kurrë të mos janë takuar.

Sot, kur Interneti përdoret më tepër se vetëm për shpërndarjen e informatës, bizneset duhet të përdorin mekanizma të sigurt dhe të besueshëm për bartjen e të dhënave. Trendët aktual, implementojnë sigurinë në cilësinë e protokollit që qëndron në mes të TCP-së dhe aplikacioneve për rrjetë. Shembuj të një qasjeje të këtillë janë Secure Socket Layers (SSL) dhe Transport Layer Security (TLS). SSL është një protokoll i uebit që vendos sesion të sigurt në mes të shfletuesit të

klientit dhe serverit të uebit. SSL i zhvilluar nga Netscape dhe pastaj i dhuruar deri tek IETF për standardizim, enkripton të gjitha të dhënat që bartën në mes të klientit dhe serverit të uebit në nivelin e IP socket. SSL së bashku me HTTPS ofrojnë siguri për tregti elektronike, përfshi këtu mbrojtjen nga përgjimi dhe ngatërrimi i të dhënave. Në anën tjetër, TLS konsiderohet një pasardhës i SSL, paraqet një protokoll tjetër kriptografik që ka për synim të ofron komunikime të sigurta në Internet. Si edhe SSL, edhe TLS ofron mbrojtje nga përgjimi dhe ngatërrimi i të dhënave, përfshi këtu edhe falsifikimin e tyre. Sërish është Netscape që bëri zhvillimin e TLS dhe pastaj i dhuroi IETF-së për standardizim.

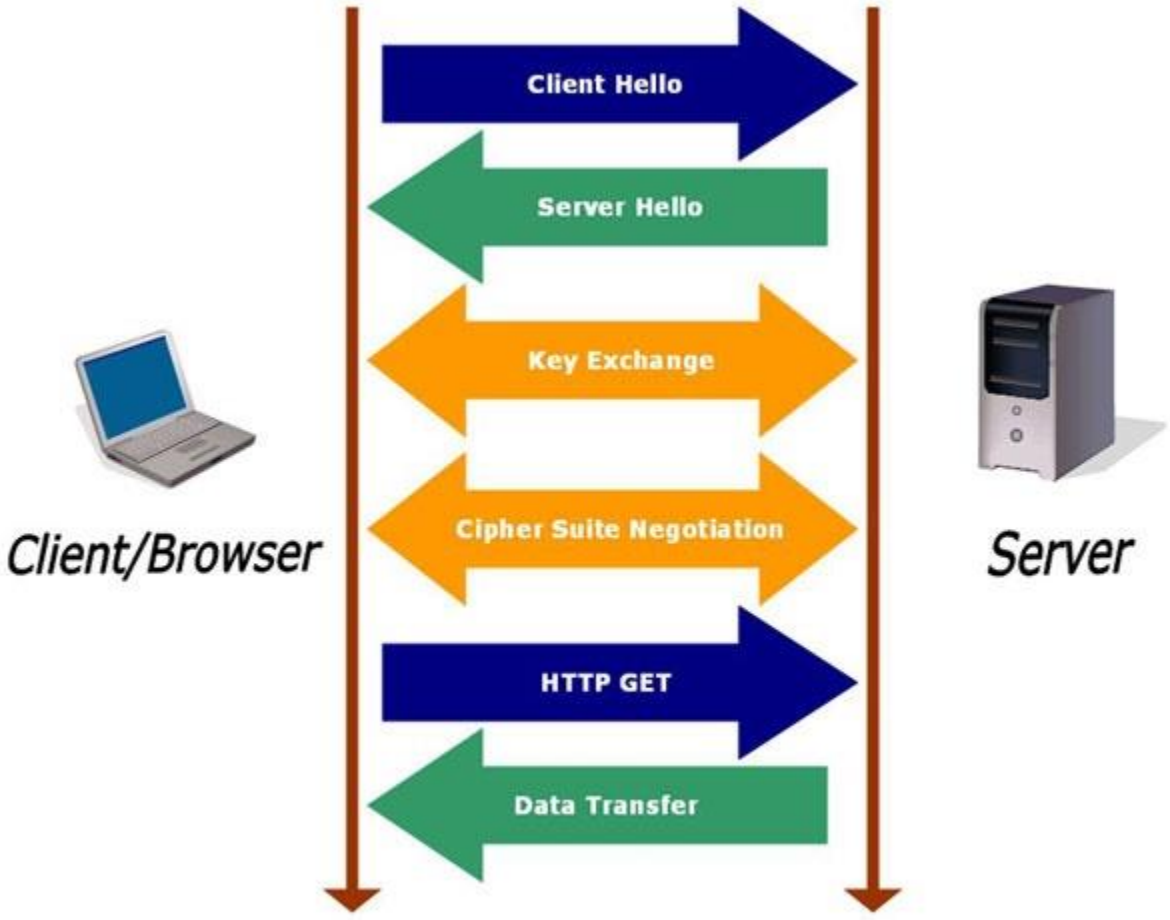


Figura 5. Principi i punës së SSL (adgrafics, 1997- 2009)

Protokolli i natyrshëm për komunikim në mes të shfletuesit të klientit dhe serverit të uebit është Hypertëxt Trasnfer Protocol (HTTP). HTTP është ideal për komunikime të hapura, megjithatë nuk ofron elementë të autentikimit dhe të enkriptimi. Në vend të saj, HTTPS përdoret

për komunikim të sigurt në mes të shfletuesit të klientit dhe të serverit të uebit. HTTPS është shumë i dobishëm për enkriptimin e të dhënave të bazuara në formularë që bartët nga shfletuesi i klientit e deri tek serveri i uebit. HTTP sipër SSL, është një emër dhe mënyrë tjetër e HTTPS, sepse i referohet kombinimit të bashkëveprimit të zakonshëm të HTTP-së sipër SSL apo TLS-së. Në këtë mënyrë, HTTPS enkripton vetëm të dhënat në nivelin HTTP të shtresës së aplikacionit, ndërsa SSL enkripton të gjitha të dhënat që bartën në mes të shfletuesit të klientit dhe serverit të uebit në nivelin e IP socket. Ashtu si edhe SSL dhe TLS, edhe HTTPS është zhvilluar nga Netscape.

E ardhmja e Kriptografisë

Me aplikimin e kompjuterëve kuantik, kriptografia do të gjente akoma më shumë zbatim se sa që përdoret sot. Është interesant fakti që aplikacioni i parë i kompjuterit kuantik të ditëve të sotme i përket fushës së enkriptimit, ku një kod enkriptimi i rëndomtë (dhe me i mirë), i njohur si RSA bazohet kryesisht ne vështirësitë e faktorizimit të numrave të mëdhenj të përbërë në primet e tyre. Kështu, po që se kompjuterët kuantik një ditë bëhen realitet, atëherë ekziston potencial i madh që një transformim radikal të ndodh në fushën e kriptografisë. Kjo për faktin që natyra e kriptosistemeve ekzistuese tashmë të aplikuara në kompjuterët klasik, do të duhej të modifikohej për të qenë të përshtatshëm për aplikim dhe përdorim në llojin e kompjuterëve kuantik.

Konkluzioni

Të gjithë jemi dëshmitar, që ditë e më shumë softuerët për enkriptim të të dhënave personale dhe avancim të intimitetit po bëhen gjithnjë e më të rëndësishëm dhe me interes për përdoruesin e rëndomtë. Natyrisht, këto aplikacione po mundësojnë qasje, bartje dhe ruajtje më të sigurt të të dhënave. Me dashje ose pa dashje, realiteti aktual në Internet dhe kudo ne rrjetë kompjuterike po ndikon që në nivelin e përdoruesve përdorimi i aplikacioneve të bazuar në kriptografi të bëhet standard.

Kapitulli 4: Kriptografia ndërkombëtare

"Kriptografia është shkencë ndërkombëtare." Bruce Schneier

Kriptografia ka ekzistuar qe nga zanafilla e njerëzimit. Thënë ndryshe, që kur njerëzimi filloi të komunikoj u paraqit nevoja që ta fshehë një pjesë të komunikimit. Përgjatë historisë, kriptografia më shumë është konsideruar si art se sa një disiplinë shkencore. Kjo për faktin që edhe pse metodat matematikore luajnë rol me rendësi ne kriptografi, sërish ajo nuk bazohet vetëm në funksionet matematikore. Sot, përveç ushtrisë dhe shërbimeve inteligjente kriptografinë e përdorin me të madhe organizata të tjera. Kriptografia është bërë një teknikë e zakonshme e komunikimit në mes të individëve, grupeve, organizatave dhe korporatave, kjo ngaqë komunikimi i informatës është bërë më i rëndësishëm dhe më me vlerë se kurdo herë më parë. S'ka dyshim se politikat dhe standardet e ndërlidhura me kriptografinë ne mënyrë të dallueshme do ta ndryshojnë të ardhmen e teknologjisë së kriptografisë. Në rreshtat në vijim do të përmendim disa nga organizatat ndërkombëtare më me influencë në vendosjen e standardeve në teknologjinë e kriptografisë.

Standardet

Historia e standardizimit të kriptografisë nuk është shumë e vjetër në krahasim me vetë historinë e kriptografisë. Përderisa ditë e më shumë teknologjitë moderne po depërtojnë në jetët tona, industritë ndiejnë nevojën për kontrollimin e këtyre teknologjive ashtu që ato të jenë në pajtueshmëri me produktet e prodhuesve të ndryshëm në mënyrë që përdoruesit të mos ndjehen konfuz dhe të parehatshëm. Sot, në epokën e informatikës, informata ndodhet kudo dhe rrjedh gjithë e andej linjave të komunikimit publik dhe privat.

Standardizimi është proces që përfshinë inicimin, zhvillimin dhe aplikimin e akteve të standardeve. Me një fjalë, është proces që bashkon hulumtimet shkencore dhe përvojën aplikative ne përcaktimin e saktë të kërkesave të favorshme teknike ne lidhje me orientimin e teknologjisë. Rezultati i këtij bashkimi është një dokument autoritar i quajtur "standard". Qeveritë, industritë, dhe organizma të tjerë japin kontribut të madh në definimin dhe përcaktimin e standardeve të numërta të kriptografisë. Disa nga këto organizata janë: ISO, IEEE, ANSI, NIST, dhe IETF.

Organizatat për standardizimin e Kriptografisë

Internet Engineering Task Force (**IETF**) është përgjegjëse për zhvillimin e standardeve dhe protokolleve aktuale dhe të reja në Internet, si dhe publikimin e Request for Comments (RFC). IETF është një komunitet ndërkombëtar i madh dhe i hapur i përbërë nga projektues të rrjeteve, operatorëve, prodhuesve, dhe hulumtuesve të cilët për objektivë kanë evoluimin dhe funksionimin e arkitekturës së Internetit. Në sektorin e sigurisë, IETF përmban shumë grupe punuese siç janë: Kerberos, IPSec, X.509, S/Mine dhe TLS, të cilat merren me standardizimet e kriptografisë dhe mirëmbajtjet e tyre.

Isntitute of Electrical and Electronics Engineers (IEEE) thuajse si çdo organizatë tjetër me përgjegjësi në përcaktimin e standardeve, edhe IEEE është organizatë jo-profitabile e themeluar në vitin 1963. Mjafton të përmenden teknologjitë e komunikimit 802.3 dhe 802.11 dhe të kuptojmë faktin që IEEE është një nga shtytësit kryesor në bërjen e standardeve. Ne mesin e presidentëve të merituar të IEEE ishte edhe Alexander Graham Bell i cili i dhuroi njerëzimit inovacionin e telefonit si një nga mjetet për komunikim direkt në distancë. IEEE e shoqëruar nga 38 organizma të tjerë të specializuar në fusha të ndryshme teknike, vazhdon të jetë promotori kryesor në avancimin e inovacioneve teknologjike nga fusha e elektricitetit.

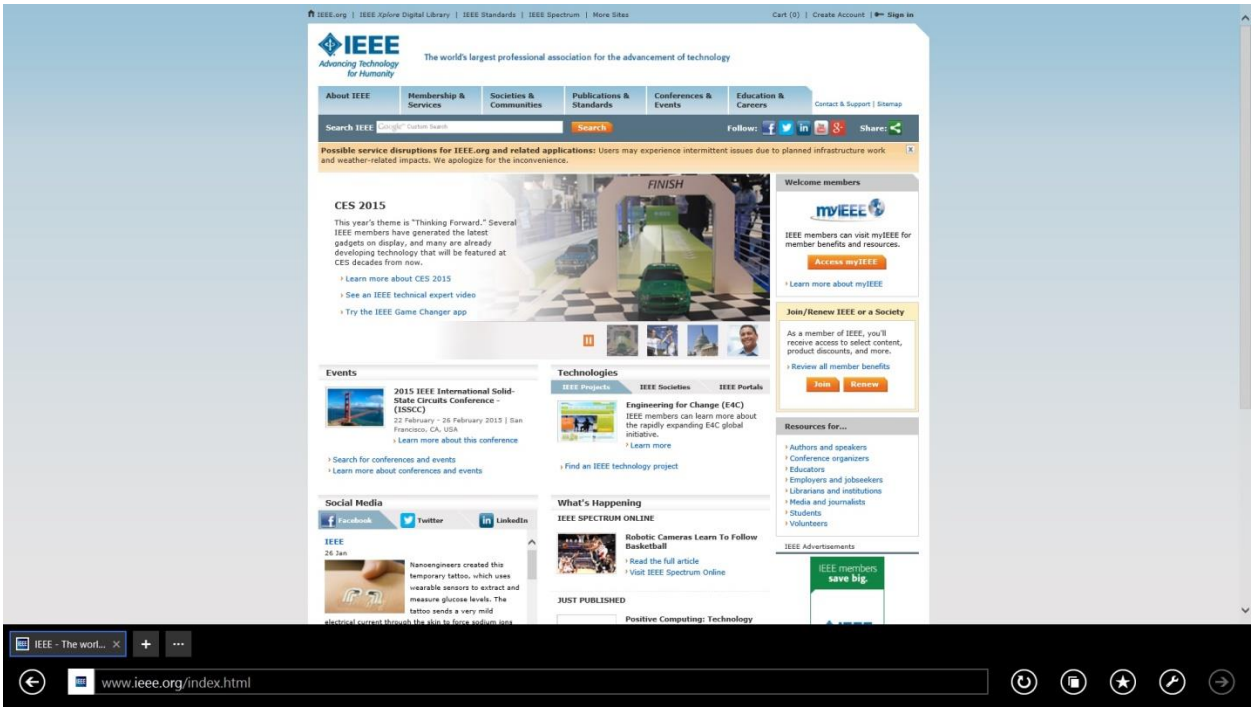


Figura 1. Ueb faqja e IEEE-së

National Institute of Standards and Technology (NIST) u themelua më 1901. NIST është agjenci federale jo-rregullative pjesë e Administrimit të Teknologjisë në Departamentin e tregtisë të ShBA. Misioni i NIST është zhvillimi dhe promovimi i masave, standardeve dhe teknologjive për avancim të produktivitetit, lehtësimit të tregtisë dhe përmirësimit të kualitetit të jetesës. Standardet e NIST nxjerrën në formë të Federal Information Processing Standards (FIPS). Disa nga standardet e rëndësishme janë: Data Encryption Standard (DES) më 1977, Computer Data Authentication më 1985, Secure Hash Standard (SHS) më 1995 dhe 2001, Digital Signature Standard (DSS) në vitin 2000 dhe Advanced Endryption Standard (AES) në 2001.

The American National Standards Institute (ANSI) e themeluar më 1919, është organizatë privatë jo profitabile që administron dhe koordinon sistemin për standardizim vullnetar dhe vlerësim e pajtueshmërisë të ShBA. Një nga komitetet e ANSI është edhe ANSI X9 që merret me zhvillimin e standardeve për industritë financiare, më konkretisht me menaxhimin e numrit për identifikim personal (PIN) procedimin e çeqeve si dhe të transfertave elektronike të parave.

International Organization for Standardization (ISO) është një organizëm jo qeveritar misioni i së cilës është promovimi global i zhvillimit të standardeve. ISO përbëhet nga rreth 1700 komitete, nën komitete dhe grupe punuese teknike. ISO/IEC zhvilloi standardin ISO/IEC 9798 për teknikat e autentikimit të entiteteve. Pastaj, standardin ISO/IEC 9796 për skemën nënshkrimit digjital që mundëson restaurimin e mesazhit. Standardi ISO/IEC 9594-8 përcakton llojin më të përdorur të certifikatave me çelës publik. Ndërsa, standardi ISO/IEC 9979 përcakton procedurat për regjistrimin e algoritmeve për kriptografi.

Kontributi i standardeve

Pa organizatat për standardizim ne vendosjen e standardeve minimale të performancës do të mbretëronte kaos dukshëm më i madh në botë se sa ky që aktualisht ekziston. I gjithë qëllimi i këtyre organizatave është që industria ti përmbahet udhëzimeve pa përjashtime. Shpesh pa nevojë humben jetë, liri, kohë, energji dhe para sepse standardet nuk janë zbatuar pa ndonjë konsideratë të arsyeshme. Standardet mund të përmirësojnë duke definuar qartë se çfarë duhet të

dizajnohet dhe çfarë performance mund të pritët. Në lidhje me kriptografinë, standardet mund të sigurojnë:

- Mbrojtje nga zgjidhjet jo të sigurta të regjistruara
- Ndërveprimin
- Emërtuesin e rëndomtë për sigurisë

Standardet e kriptografisë ndihmojnë në përcaktimin e algoritmeve, protokolleve të komunikimit, formatit të të dhënave, kualitetit të harduerit dhe softuerit dhe trajtimit të të dhënave të ndërlidhura me sigurinë. Standardet u ndihmojnë përdoruesve që të dinë se çfarë kushtesh specifike do të jenë të nevojshme që të plotësojnë kërkesat e tyre.

Konkluzioni

Të gjithë jemi dëshmitar, që dit e më shumë softuerët për enkriptim të të dhënave personale dhe avancim të intimitetit po bëhen gjithnjë e më të rëndësishëm dhe më me interes për përdoruesin e rëndomtë. Natyrisht, këto aplikacione po mundësojnë qasje, bartje dhe ruajtje më të sigurt të të dhënave. Me dashje ose pa dashje, realiteti aktual në Internet dhe kudo ne rrjetet kompjuterike po ndikon që në nivelin e përdoruesve përdorimi i aplikacioneve të bazuar në kriptografi të bëhet standard. Në këtë mënyrë kriptografia nuk ndalon në kufijtë kombëtar! Kjo bënë që hulumtimet, standardet, dhe produktet të jenë ndërkombëtare. E me këtë, edhe ekspertiza të bëhet ndërkombëtare.

Kapitulli 5: Intimitet Goxha i Bukur (PGP)

"Mjeshtëria e vërtetë e dialogut nuk është vetëm të thuash fjalën e duhur në vendin e duhur, por ta lësh të pa thënë fjalën e gabuar ne momentet tunduese." Lady Dorothy Nevill

Në ditët e sotme, kur thuajse shumica e aktiviteteve me kompjuter realizohen duke qenë të lidhur në Internet, krahas sjelljes tonë së qënurit në-linjë shumë e rëndësishme është dhe ruajtja e intimitetit. Janë të shumtë raportet e sigurisë së rrjeteve dhe sistemeve kompjuterike që flasin për shkelje të intimitetit. Pa dyshim, këto raporte nuk kursejnë as rrjetet sociale si Facebook, Twitter, MySpace, dhe të tjera. Po ta shikojmë këtë problematik nga këndvështrimi i biznesit, vërejmë se bizneset janë shumë të shqetësuar me shkeljen e intimitetit sepse kjo për ta do të thotë me pak tregti elektronike. Ndërsa kur e shikojmë nga këndvështrimi i përdoruesit edhe pse shqetësimi duket të mos jetë në nivelin e biznesit, sërish tema e intimiteti në Internet sikur synon të zë një nga vendet e para të shqetësimeve të përdoruesve. Pavarësisht, një gjë është më se e sigurt që industria e teknologjisë informative ditë e më shumë po bëhet më e vetëdijshme me problemin e intimitetit në Internet, me çka edhe i tërë potenciali i saj zhvillimor si në harduer ashtu edhe në softuer është orientuar kah realizimi i mekanizmave për ta bërë lundrimin në Internet sa më të sigurt. Me këtë edhe jetën në Internet, si një botë virtuale, sa më të shëndetshme.

Hyrje: Pretty Good Privacy (PGP)

Pretty Good Privacy apo PGP siç edhe i referohen shpesh është një softuer me anë të së cilit bëhet shifrimi i të dhënave për tu transmetuar pastaj përmes postës elektronike. I shpikur nga Phil Zimmerman, ky intimitet goxha i bukur krahas shifrimit të postës elektronike mundëson edhe ruajtjen e integritetit të tyre. Fillimisht një produkt pa pagesë, komercializohet në mesin e viteve të '90-ta kur blihet nga Network Associates. Pastaj pronar të PGP ishte PGP Corporation, ndërsa tanimë është Symantec që ka blerë këtë teknologji. Symantec ofron më shumë se vetëm shifrimin dhe integritetin e të dhënave të postës elektronike. Siguria e të dhënave të përdoruesve të skajshëm, siguria e postës elektronike, autentikimi në rrjetet e reve dhe shumë të tjera paraqesin disa nga produktet e sotme që ofron PGP Corporation në rrafshin e sigurisë kompjuterike. Megjithatë, të gjithë të interesuarit e PGP mund të shkarkojnë edhe versionet pa

pagesë nga Interneti ndërsa me mundësi përdorimi për kohë të caktuar nga faqja e uebit të PGP Corporation:

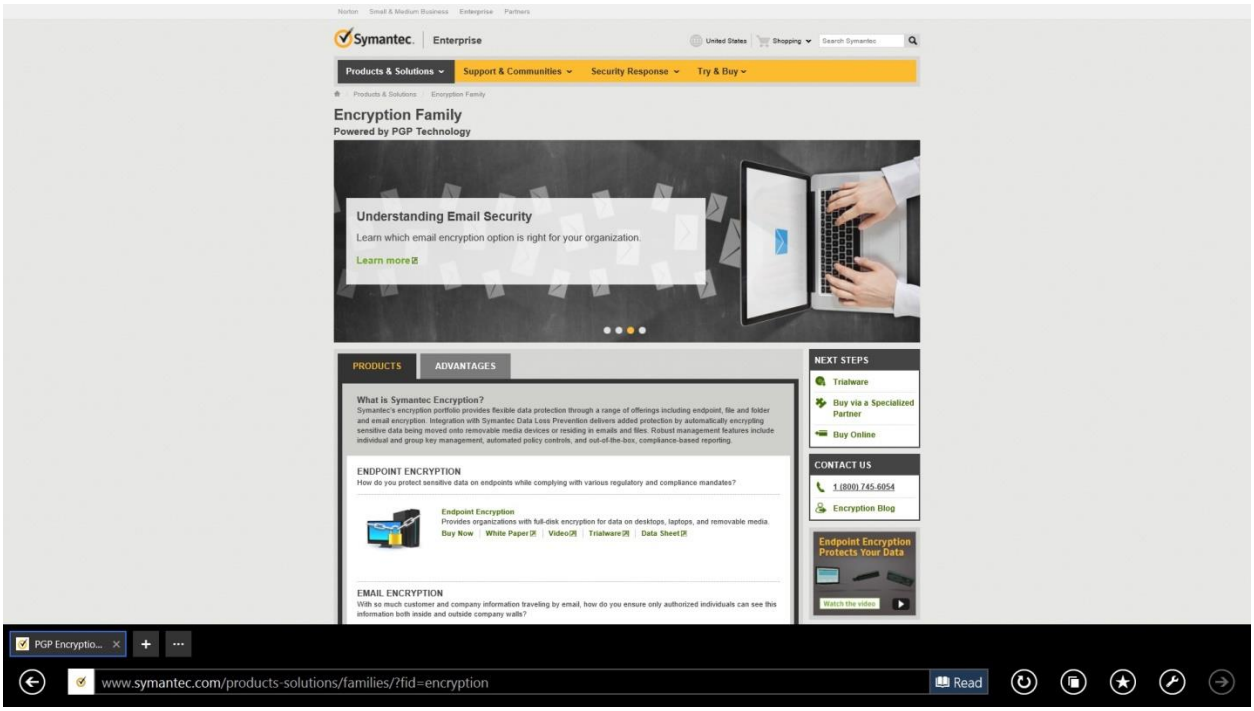


Figura 1 Faqja e uebit të Symantec

PGP në aksion

PGP punon në principin që para se të dërgohet e dhëna e besueshme përmes postës elektronike, fillimisht duhet të shifrohet kjo e dhënë me PGP e pastaj të dërgohet përmes postës së rëndomtë elektronike. Thuajse në mënyrë të ngjashme, në skajin tjetër të rrjetës kompjuterike përdoruesi që tanimë ka pranuar mesazhin me këtë të dhënë të besueshme do të duhet së pari ta përdorë PGP për të bërë deshifrimin e mesazhit ashtu që pastaj të jetë në gjendje ta përdorë atë. Sa i thjeshtë, aq edhe i papërshtatshëm! Por, duke qenë se kodi burimor i PGP është i pajisur me modifikimet e nevojshme për të bërë të mundur pajtueshmërinë dhe përfshirjen e këtij softueri në sistemet e ndryshme të postave elektronike, praktika ka dëshmuar se PGP shumë lehtë bëhet pjesë përbërëse e aplikacioneve të postave elektronike të përdoruesve.

Varësisht se a është zgjedhur besueshmëria, integriteti, autentikimi apo ndonjë kombinim i ndonjërës nga këto, PGP ekzekuton aksionet ne vijim:

- Krijon çelësin e sesionit të rastit për algoritmin simetrik.
- Shifron mesazhin me ane të çelësit të sesionit (për besueshmëri të mesazhit).
- Shifron çelësin e sesionit sipas çelësit publik të pranuesit.
- Bën shifrimin e mesazhit dhe klasifikimin e tij; e firmos shifrimin e mesazhit me çelësin e shifruar privat të dërguesit (për integritet dhe autenticitet të mesazhit).
- Ia bashkangjet çelësin e shifruar të sesionit mesazhit të shifruar dhe të klasifikuar.
- E transmeton mesazhin deri të dërguesi.

Avantazhet e PGP

Zimmerman është i bindur se avantazhet e PGP, që fillimisht ishte zhvilluar si projekt për të drejtat e njeriut për ti mbrojtur individët nga qeveritë tiranike, i tejkalojnë disavantazhet. Zaten edhe kjo mund të jetë një nga arsyet që PGP përdoret nga çdo organizatë për të drejtat e njeriut në botë. Disa nga avantazhet e PGP janë:

- PGP është i lehtë për tu përdorur.
- Me PGP secili përdorues vendos se cilit çelës duhet ti besojë.

Certifikatat janë opsionale në PGP, që do të thotë se secili mund ti lëshoj certifikatë secilit, dhe është përdoruesi ai që vendosë se cilës certifikatë duhet ti besojë për të autentikuar dikë.

Gjatë deshifrimit të të dhënave me PGP, ju mundësohet të përcaktoni se e dhëna është skedarë tekstual apo binar.

Me qëllim të kursimit të bitëve, PGP ndrydh skedarin para se ta dërgojë atë pavarësisht se a është tekstual apo binar.

Figura 2 PGP Global Directory për verifikimin e çelësave

Disavantazhet e PGP

Për dallim nga avantazhet, ekzistojnë edhe disa avantazhe të PGP si në vijim:

- PGP në secilin mesazh përfshin edhe fushën EMRI I SKEDARIT.
- PGP përfshinë kohën kur herën e fundit skedari është modifikuar.
- PGP lejon të përdorët çfarëdo emri, duke shkaktuar kështu që përdoruesit të firmosin certifikatat sikur të jenë çelësa publik.
- PGP nuk supozon se gjithnjë skedari i shifruar duhet të kodohet për tu dërguar me postë elektronike.
- PGP nuk kërkon përdorimin e certifikatave, edhe pse ato e lehtësojnë punën me sistemet e sigurisë së intimitetit.

Konkluzioni

PGP mund të konsiderohet një protokoll tjetër i sigurt i postës elektronike. Nisi si implementim në domenin publik të vetëm, për tu shpërndarë pastaj në gjithë botën. Mjerisht,

ishte RSADSI dhe autoritetet qeveritare që i shkaktuan PGP të kalojë në kontrabandë. Për ironi, që nga fillimi PGP ka qenë legal dhe në dispozicion në shumë vende të botës. Duke qenë se patenta e RSA vlente vetëm për ShBA dhe fakti që shtetet tjera kanë politika tjera të importit, eksportit dhe përdorimit të teknologjive për siguri të intimitetit, legaliteti i PGP mbeti pothuajse gjithnjë i diskutueshëm. Pavarësisht, PGP me natyrën e saj të intimitetit goxha të bukur edhe përkundër problemeve të ndërlidhura me ligjshmërinë e përdorimit të saj, sërish anë e mbanë botës inspiroi përdorues të shumtë të cilët e përdorën për të përkrahur liritë individuale të tyre, krenaritë prej eksperti dhe dëshirat e tyre për të qenë të pavarur nga nevoja për çfarëdo fshehtësie.

Kapitulli 6: IPS përballë IDS

"Kur njeriu drejton gishtin kah tjetri, ai duhet të kujton që katër gishtat e dorës së tij janë të drejtuar kah vetja e tij." Louis Nizer

Duke u bazuar në fjalinë e urtë "*parandalimi është më i mirë se shërimi*", atëherë shumë lehtë do të mund të krahasoheshin sistemet për parandalim të ndërhyrjeve (IPS) me sistemet për detektim të ndërhyrjeve (IDS). Përderisa, sistemet IDS mbrojtjen e të dhënave, aplikacioneve dhe shërbimeve e bazojnë në detektimin e trafikut të dyshimtë dhe për të cilën njoftojnë administratorin e rrjetit; sistemet IPS bazohen në qasjen proaktive duke e krahasuar gjendjen aktuale të trafikut në rrjet me politikën dhe rregullat e sigurisë të kompanisë me çka jo vetëm që e njofton administratorin e rrjetit por edhe ndërmerr hapa konkret drejt evitimit të një sulmi të mundshëm. Teknologjia e sistemeve për parandalim të ndërhyrjeve (IPS) po sheshohet ditë e më shumë, duke u bërë kështu një teknologji bindëse kur bëhet fjalë për përdorim të teknologjive për sigurinë e rrjeteve kompjuterike.

Historiku i sistemeve IPS

Pavarësisht se sulmi mund të jetë një aktivitet i qëllimtë dhe i organizuar mirë që vjen nga jashtë apo një aktivitet i paqëllimtë dhe jo i organizuar mirë qe vjen nga brenda, sistemet për detektimin e ndërhyrjeve (IDS) vlerësohen të jenë teknologji pasive ne mirëmbajtjen e sigurisë së rrjetit kompjuterik. Kjo për faktin që IDS merret me "detektimin" e sulmit dhe jo "parandalimin" e tij! Për të tejkaluar këtë situatë të sigurisë pasive në fillim të viteve 90-ta u prezantuan sistemet për parandalimin e ndërhyrjeve (IPS). Ishte Andrew Plato (konsulent i Network ICE) i cili për here të pare përdori termin Intrusion Prevention System (IPS). Sot, përderisa disa nga ekspertët e sigurisë së rrjeteve kompjuterike e shohin IPS si zgjerim i IDS, shumica e pranojnë faktin që IPS vërtetë është zgjidhje proaktive e sigurisë. Ne Figurën 1 është paraqitur interesimi në rritje për implementimin e pajisjeve IPS ose zgjidhjeve IPS për të siguruar hostet dhe infrastrukturën e rrjeteve kompjuterike.

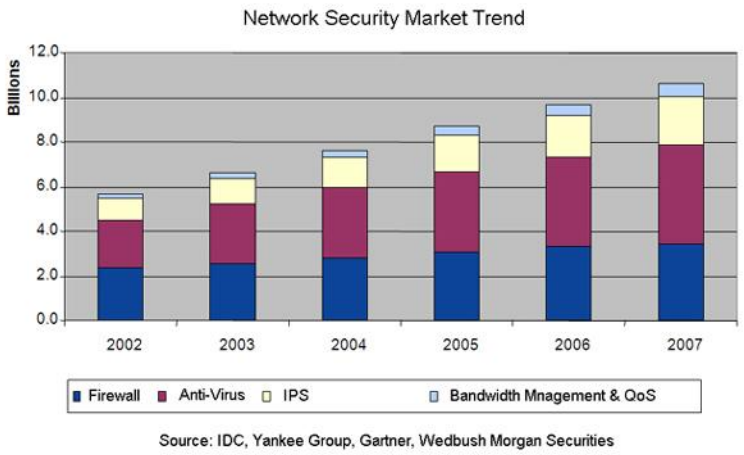


Figura 1. Trendi i tregut për siguri të rrjeteve (Xuhua Ji, Shtator 2007)

Llojet e sistemeve IPS

Meqë prejardhja e sistemeve IPS është nga sistemet IDS, atëherë përmbajnë ngjashmëri të shumta kur behet kategorizimi i llojeve të përdorshme të tyre. Ne këtë mënyrë, IPS ndahet ne dy lloje:

1. **Sistemet IPS të bazuara ne hoste (HIPS)** është teknologji e re e cila bazohet në agjentët e sigurisë të cilët instalohen nëpër serverë dhe stacione pune. Ne bashkëpunim me kernellin e sistemit operativ dhe shërbimet, monitoron dhe kap trafikun e dyshimtë me qellim të parandalimit të sulmit. Nëse një organizatë ka bërë implementim të duhur të sistemeve HIPS në hostet e perimetrit të rrjetit të brendshëm të saj, përfitimet janë si vijon:

- Parandalim i sulmit
- Asistencë në arnim
- Parandalim i përhapjes të sulmeve të brendshme
- Përforcim i politikës së sigurisë

Meqë asnjë teknologji nuk është ideale, e njëjta gjë vlen edhe për sistemet HIPS. Disa nga disavantazhet e saj janë:

- I ekspozohen ngacmimeve të përdoruesve
- Mungesë e sigurisë së plotë
- Mos parandalim i sulmeve që nuk kanë në objektivë hostet

Edhe pse sistemet HIPS janë dëshmuar të jenë zgjidhje e duhur e sigurisë kompjuterike, serish jo të gjitha organizatat kanë mundësinë e implementimit të tij. Fakti që agjentët e sistemit HIPS duhet të instalohen në të gjithë serverët dhe stacionet e punës së organizatës, e që në ndërmarrje kjo arrin shifrën ne mijëra sosh, atëherë kostoja e implementimit të sistemit HIPS behet shume e lartë.

Figura 2. Sistemet (NetworkD, pa datë)

2. Sistemet IPS të bazuara në rrjet (NIPS) janë një zgjidhje alternative nga ato të sistemeve HIPS, të cilat kanë për synim vendosjen e sigurisë në infrastrukturën e rrjetit dhe jo në hoste. Në përmbajtje janë kombinim i sistemeve standarde IDS, IPS dhe mureve mbrojtës të rrjetit, me çka edhe nganjëherë njihen si IDS të brendshëm ose Gateway IDS. Ne përgjithësi monitorojnë trafikun që hyn dhe del nga rrjeti, respektivisht ekzaminojnë anomalitë e protokolleve, komandat që zakonisht nuk ekzekutohen në rrjet dhe shumë aktivitete të tjera që kanë për synim jo funksionalitetin e infrastrukturës së rrjetit. Nëse një organizatë ka bërë implementim të duhur të sistemeve NIPS në infrastrukturën e perimetrit të rrjetit të brendshëm të saj, përfitimet janë si vijon:

- Normalizim i trafikut
- Përforcim i politikës së sigurisë

Kur bëhet fjalë për të metat teknologjike, atëherë edhe sistemet NIPS nuk janë pa to! Në vijim po përmendim disa nga disavantazhet e saj:

- Sistemet NIPS nuk janë te përkryera
- Ndikojnë në efektivitetin e rrjetit

Duke ditur tashmë fuqinë mbrojtëse të llojeve të sistemeve IPS si dhe të metat e tyre teknologjike, në praktikë kemi situata kur implementohen:

- Vetëm sistemet HIPS,
- Vetëm sistemet NIPS (zgjidhje që implementohet më së shpeshti) ose
- Ne formë të kombinuar – sistemet HIPS dhe NIPS së bashku (zgjidhje shumë e shtrenjtë).

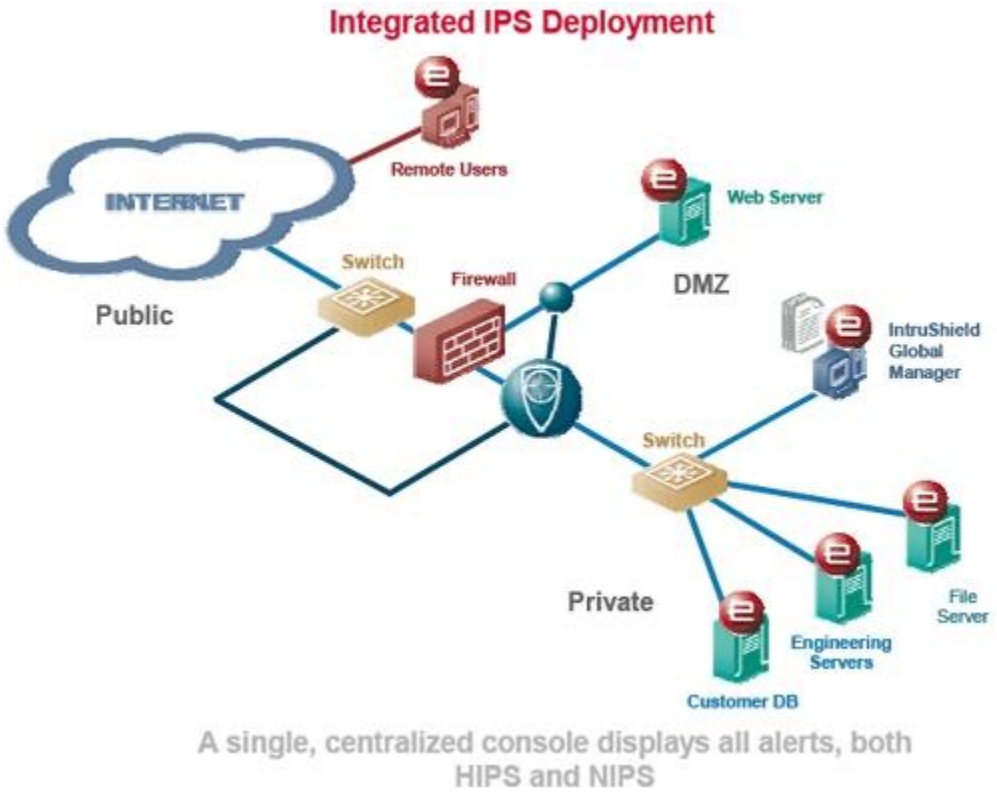


Figura 3. Sistemet HIPS dhe NIPS së bashku (SecureSynergy, pa datë)

IPS përballë IDS:

Beal kur bënë krahasimin e sistemeve IPS me ato IDS thekson se "*është si ti krahasosh mollët me portokajtë*". Edhe pse që të dy këto teknologji janë teknologji që synojnë të vendosin sigurinë në rrjetet kompjuterike, serish dallimet janë të shquara. Po fillojmë si në vijim:

Sipas definicionit: përderisa IDS ekzaminon paketat, mbledh dhe dokumenton informatat dhe alarmon administratorin e rrjetit se diçka e çuditshme po ndodhe në rrjet, në anën tjetër IPS përveç qe bënë ekzaminimet që i bën IDS, gjithashtu ne mënyrë automatike ndalon trafikun të cilin e vlerëson si papërshtatshëm ose keqbërës.

Mosha: nëse merren për bazë periudhat kohore të paraqitjes së këtyre teknologjive të sigurisë, IDS mund të quhet vëlla i madhë i IPS.

Qasja: përderisa IDS bazohet më shumë në qasjen "***detekto dhe pastaj merru me te***" gjë që e bën të jetë zgjidhje pasive e sigurisë, IPS preferon qasjen proaktive "***parandalimi është me i mire se shërimi***" me çka e bën të jetë zgjidhje aktive e sigurisë.

Besueshmëria: IDS duke qenë teknologji më e vjetër në moshë se sa IPS, tashmë ka arritur një besueshmëri të konsiderueshme në krahasim me IPS që është teknologji më e re në moshë dhe më pak e njohur.

Përfitimet: ne bazë të raporteve del që IPS dëshmon të ofrojë më shumë përfitime për organizatat sesa IDS dhe kjo falë tiparit intuitiv të IPS në vendosjen e sigurisë në rrjetet kompjuterike.

Kostoja: kur vjen puna tek implementimi IDS vazhdon të mbetet teknologji më e lirë në krahasim me IPS që mbi supet e veta vazhdon te bartë një kosto të lartë të implementimit.

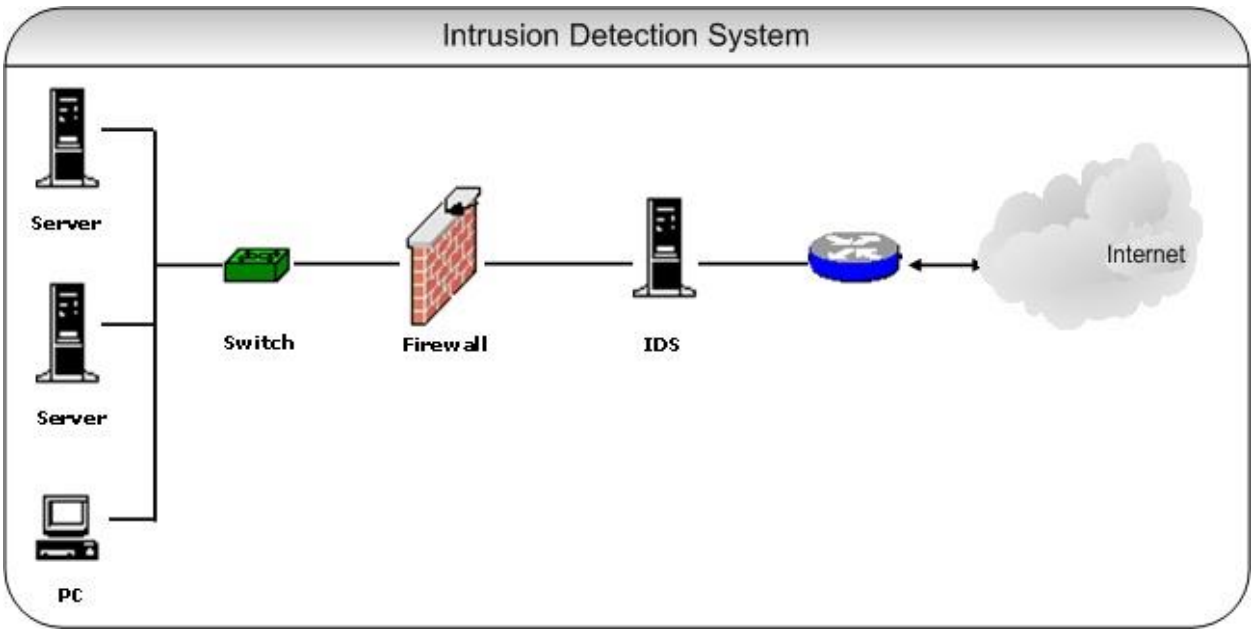


Figura 4. Sistemi IDS (Brown, Cocks, dhe Swampillai, Shkurt 2004)

Procesi i implementimit te IPS

Procesi i implementimit të sistemit IPS varet shumë nga lloji i zgjedhur për parandalimin e ndërhyrjeve. Në bazë të kësaj, procesi i implementimit të IPS është si vijon:

Shpërndarja e pajisjeve IPS: pavarësisht nga konfiguracioni i rrjetit tuaj, topologjia dhe modeli i trafikut ju duhet të analizoni shpërndarjen e pajisjeve IPS nga dy perspektiva:

1. Sistemet IPS të bazuara në hoste (HIPS): kërkojnë instalimin e agjentëve të sistemit HIPS në secilin host te rrjetit tuaj kompjuterik dhe
2. Sistemet IPS të bazuara në rrjet (NIPS): kërkojnë shpërndarjen e NIPS gjithë andej infrastrukturës fizike të rrjetit kompjuterik ashtu që të inspektoj trafikun e brendshëm dhe të jashtëm.

Konfigurimi i pajisjeve IPS: disa nga faktorët që duhet konsideruar janë:

1. Akordimi i nënshkrimeve: kërkon akordimin e nënshkrimeve specifike të cilat do gjenerojnë pohues te pavërtetë në rrjetin tuaj
2. Reagim në ndodhi: kërkon konfigurimin e secilit nënshkrim ashtu që të gjeneroj një ose më shumë nga aksionet vijuese: moho, alarmo, ndalo ose dokumento.
3. Përditësimin e softuerit: kërkon aktivizimin e këtij tipari ashtu që softueri i IPS tuaj të jetë i përditësuar në mënyrë që njëmend të jetë rrjeta juaj e sigurtë.
4. Dështimi i pajisjes: kërkon konfigurimin e kësaj veçorie ashtu që të dihet paraprakisht çfarë do të ndodhe nëse pajisja e IPS ka probleme.

Monitorimi i aktiviteteve te IPS: kur të planifikoni strategjinë e monitorimit, duhet pas në kujdes faktorët në vijim:

1. Metoda e menaxhimit: zakonisht dy metoda të menaxhimit janë në dispozicion: individuale dhe e centralizuar.
2. Korrelacioni i ndodhisë: i referohet procesit të lidhjes reciproke të sulmeve dhe ndodhive të tjera që ngjajnë në pika të ndryshme në rrjetin tuaj përfshi këtu edhe sulmet e shumëfishta që ndodhin në të njëjtën kohë.

3. Personeli i sigurisë: përgjegjës për të ekzaminuar alarmet e numërta dhe ndodhi të tjera të gjeneruar nga IPS gjatë procesimit të trafikut të rrjetit tuaj.
4. Plani për reagim ndaj incidentit: në rast se rrjeti juaj është sulmuar, kërkohet përpilimi i një plani në të cilin do të specifikoni hapat e reagimit tuaj.

Sigurimi i komunikimeve të IPS: në përgjithësi komunikimet e IPS bëjnë pjesë në dy kategori :

1. Komunikimet e menaxhimit: ekzistojnë dy opsione për të realizuar komunikime të sigurta: menaxhimi jashtë-brezit dhe protokollet e sigurta.
2. Komunikimet pajisje-me-pajisje: kërkon që pajisjet tuaja të IPS të komunikojnë me njëra tjetrën ose me pajisjet tjera të infrastrukturës së rrjetit.

Po të shikosh të gjitha hapat që duhet të ndërmerren për të implementuar një zgjidhje të sigurtë të rrjetit kompjuterik të bazuar në sistemet IPS, mbase mund të tingëllojë sikur "***ka shume për tu bërë***". Por, po të krahasohen të gjitha këto aktivitete të konfigurimit me përfitimet që fiton organizata në rrafshin e sigurisë, atëherë "***ja vlen barra qiranë***".

Konkluzioni

Duke marre për bazë faktin që siguria sot është aktivitet parësor për secilën organizatë sa herë që kërkohet të realizohet një rrjet kompjuterik me shërbime të caktuara, atëherë mund të llogaritet në sistemet IPS si një zgjidhje e mirë për vendosjen e sigurisë në një rrjet të tillë. Përderisa një numër i ekspertëve të sigurisë pohojnë që epoka e sistemeve IDS është në mbarim dhe se këto tashmë po zëvendësohen nga sistemet IPS, të tjerët vlerësojnë se ardhmëria është e ndritur për të dy teknologjitë e sigurisë se rrjeteve kompjuterike. Kjo për faktin sepse praktikat kanë dëshmuar se që te dy teknologjitë IDS dhe ato IPS nuk bëjnë dot pa njëra tjetrën. Ose sistemet IPS vetëm ose në formatin hibrid, një gjë është e sigurtë, në vitet qe do të vijnë do të ketë zgjerim të sistemeve IPS.

Kapitulli 7: Si punon skaneri biometrik?

"Nëse intimiteti është nxjerrë jashtë ligjit, vetëm shkelësit e saj do të kenë intimitet." – Phil Zimmermann

Në ditët e sotme, të gjithë ne po i jetojmë përfitimet e shumta që na vijnë nga pajisja e quajtur kompjuter! Pa dyshim, kompjuteri është bërë bartës kryesor i procesit të punës në shkolla, universitete, biznese, qeveri, industri, … e gjithë andej. E përdorim për të vendosur, procesuar, ruajtur, shfaqur dhe komunikuar të dhënat, funksione këto që e bëjnë kompjuterin të jetë vegël shumë praktike dhe e dobishme njëkohësisht. Me një fjalë, nuk mund të mohojmë ndikimin pozitiv të kompjuterit në jetën tonë. Përkundër të gjitha këtyre të mirave që marrim nga përdorimi i kompjuterit, njëkohësisht kjo pajisje sfidohet nga kërcënues të burimeve dhe natyrave të ndryshme, emëruesi i përbashkët i të cilëve është të vënë në rrezik sigurinë e tij (të dhënave në kompjuter). Për tu vënë në mbrojtje të kompjuterit (të dhënave në kompjuter), entuziast, profesionist dhe shkencëtarë të shumtë janë përpjekur dhe po përpiqen të gjejnë mënyra, metoda dhe vegla për të shtuar sigurinë e tij, respektivisht të të dhënave në kompjuter. Në vijim do të njihemi me skanerët biometrik si një nga teknologjitë e sotme në dispozicion për të sforcuar sigurinë e procesit të autentikimit gjatë procesit të qasjes së të dhënave në sistemet kompjuterike.

Historiku i skanerëve biometrik

Kur në vitet e 90-ta u shfaqën skanerët për regjistrimin e drejtpërdrejtë të shenjave të gishtave, ishin pajisje qe përdornin metodën e sipërfaqes së ndjeshme për të lexuar strukturën e shenjave të gishtave nga sipërfaqja e lëkurës së gishtit. Këto pajisje të hershme përdornin metodat e shëmbëlltyrës optike për të realizuar fotografimin e lëkurës së gishtave. Më pas, u përdorën mekanizma të ndryshëm të bazuar në ndjeshmëri për të detektuar strukturat në sipërfaqet e gishtave të cilat pastaj duhet të konvertohen në sinjale elektrike. Këtu u përfshinë njehsuesi infrakuq, matësi i forcës mekanike, matësi i temperaturës dhe matësi i vëllimit elektrik. Edhe pse disa nga këta mekanizma ishin të aftë të merrnin imazhet e shenjave të gishtave nga të rinjtë dhe të rriturit e shëndetshëm në ambiente të brendshme të kontrolluara, në kushte të vërteta pune të njëjtat mekanizma nuk bënin punën me sukses. Veçanërisht, nuk arrinin dot të

regjistronin imazhet e shenjave të gishtave me lëkurë të thatë, me kallo të dendur, apo të lyer lehtë nga përbërësit kimik. Dështimet e natyrës së këtillë u bënë pengesë që këto pajisje të fitojnë përdorim të gjerë.

Si punon skaneri biometrik?

Identifikimi i shenjave të gishtave është proces i krahasimit të gjurmëve të diskutueshme dhe të ditura të strukturës së vargjeve të gishtave dhe shuplakës së dorës me qëllim të përcaktimit se gjurmët janë nga i njëjti gisht apo e njëjta shuplakë. Interesant është fakti që shenjat e dy gishtave ose shuplakave nuk janë kurrë tërësisht të ngjashme (në asnjë detal të tyre), siç nuk janë të ngjashëm as edhe dy regjistrime të një pas njëshme.

Skaneri biometrik, një pajisje elektronike që luan rolin e njësisë hyrëse të kompjuterit, përbëhet nga dy komponentë kryesore: nga skaneri i shenjave të gishtave dhe softueri i shenjave të gishtave. Punon në principin që kërkon nga përdoruesi vendosjen e gishtit në skaner nga ku realizohet fotografimi i çastit. Kjo shëmbëlltyrë e krijuar quhet skanim i drejtpërdrejtë. Pastaj kjo shëmbëlltyrë përpunohet nga skaneri në një skemë të digjitalizuar të pikave të hollësishme (janë pikat me interes të shenjave të gishtit, siç janë skajet e degëzimeve dhe të vargjeve) për tu bartur tutje deri tek kompjuteri për të cilin është i lidhur. Softueri i shenjave të gishtave, ne rolin e pikës së fundme të procesit të këtillë të autentikimit, është i aftë të njohë dhe interpretojë hyrjen e pranuar nga skaneri i shenjave të gishtave. Kështu, kjo e dhënë e pranuar ruhet për tu përdorur pastaj për qëllimi krahasimi dhe autentikimi. Figura 1, tregon se si AuthenTec teknologji unike e bazuar në gjysmëpërçues për marrjen e shenjave të gishtave përdor sinjale te vogla të RF për të detektuar vargjet në strukturën e gishtit:

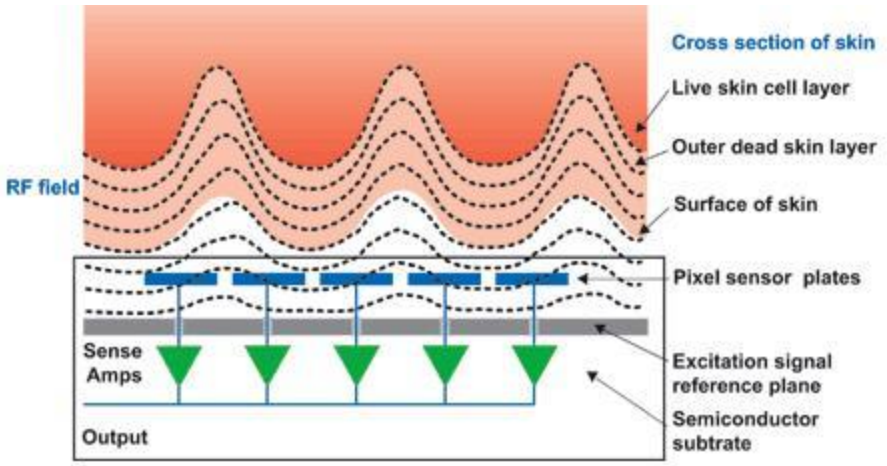


Figura 1. Teknologjia e skanerëve biometrik AuthenTec (Authentec.com, 2007)

Pavarësisht përmirësimeve në fushën e funksionalitetit, skanerët për shenjat e gishtave po përmirësohen edhe në aspektin e dizajnit. Sot, ne i hasim edhe si pjesë e integruar në tastierat e kompjuterëve PC si dhe në laptop me çka gjithnjë e më shume po bëhen pjesë standarde e konfigurimeve kompjuterike.

Teknikat e shëmbëlltyrës

Në vijim do të shohim disa nga teknikat e shëmbëlltyrës që përdoren nga skanerët biometrik:

- Optike: përdoret platforma nga xhami në të cilën vendoset gishti nga ku pastaj realizohet shëmbëlltyra e shenjës së gishtit.
- Prekje: si rezultat i presionit qe ushtron gishti ne platformën ku është i vendosur realizohet shëmbëlltyra.
- Termike: shëmbëlltyra e shenjës së gishtit realizohet nga senzori i temperaturës.
- Vëllimore: shëmbëlltyra realizohet nga senzori i silicit për vëllim.
- Ultratingull: valët zanore mund të gjenerojnë shëmbëlltyra të ultratingullit nga struktura e gishtit.

Siguria e skanerëve biometrik

Edhe pse skanerët biometrik ofrojnë saktësi të lartë dhe përpjekjet për mashtrimin e këtyre pajisjeve janë të vështira, realiteti dëshmon të kundërtën. Tsutomu Matsumoto, një kriptografist japonez, së bashku me studentët e tij nga Universiteti Kombëtar i Yokohama-së demonstroi se skanerët biometrik seriozisht mund të mashtrohen me një zgjuarsi të vogël dhe me ca pajisje shtëpiake në vlerë prej 10 USD. Matsumoto përdori xhelatinë, përbërës nga i cili prodhohen arushat e gomuar (Haribo). Eksperimenti i tij interesant bazohet ne faktin qe ai merr shenjat e gishtave të lënë në xham, pastaj të njëjtit i zmadhon me akrilat të cianurit për ti fotografuar me kamerë digjitale. Me anë të aplikacionit PhotoShop, ai përmirëson kontrastin e fotove të realizuara dhe të njëjtit i shtyp në letër të tejdukshme. Pastaj përmes një pllake të ndjeshme ndaj fotografive për shtypjen e qarqeve realizon shenjat e gishtave të gdhendura në bakër në formë tre dimensionale. Matsumoto provoi këtë eksperiment në njëmbëdhjetë skaner biometrik komercial dhe që të gjithë u mashtruan me sukses.

Konkluzioni

Sa herë që duam të sigurojmë një mjedis të caktuar për ruajtjen e të dhënave me anë të autentikimit në mënyrë të shpejtë, të lehtë dhe të lirë atëherë skanerët biometrik mund të jenë zgjidhje e parë në mesin e të gjitha teknologjive të sotme për qëllime sigurie. Ashtu siç asnjë teknologji nuk është “perfektë”, edhe skanerët biometrik nuk janë të përkryer! Edhe përkundër kompromet imit të pajisjeve të këtilla, përmirësimet dhe avancimet e bëra së fundi në këtë teknologji i bënë skanerët biometrik të jenë një nga pajisjet më të rekomanduara për siguri të dhënave në botën e sotme të digjitalizuar.

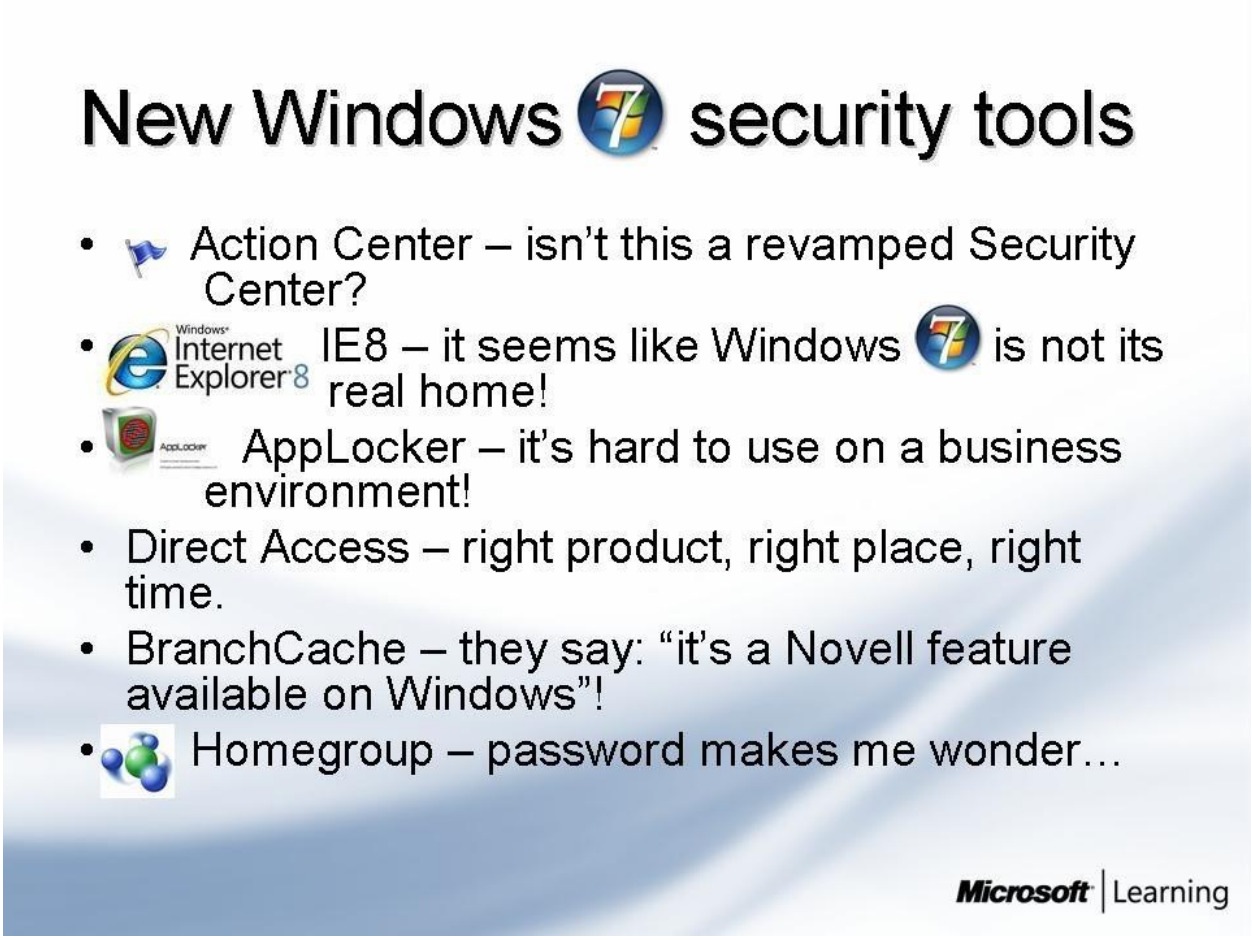
Shtojca A: A është Windows 7 i sigurtë?

"Një njeri që jeton në mënyrë të drejtë dhe është i drejtë, posedon më shumë fuqi në heshtjen e tij sesa tjetri në fjalët e tij." Phillips Brooks

A vazhdon të ketë Windows probleme me sigurinë? Mos vallë, së fundi Windows ka përmirësuar dukshëm sigurinë e tij? Apo, edhe përkundër veglërive dhe tipareve të shtuara të sigurisë, Microsoft-it do ti duhet punë për të bërë akoma më të sigurt sistemin e tij operativ! Këto dhe shumë pyetje apo komente të tjera janë vetëm disa nga ato që qarkullojnë tashmë me vite në Internet apo në çdo mjedis ku debatohet dhe diskutohet siguria e sistemeve operative te Microsoft-it përfshi këtu edhe sigurinë e Windows 7. Përmes rreshtave në vijim, nuk është qëllimi im që të rihap sërish këtë lloj të debateve apo diskutimeve, përkundrazi duke qenë se edhe vetë jam një përdorues i produkteve te Microsoft-it për vite të tëra, thjeshtë do ti bëjë një vlerësim veglërive dhe tipareve të sigurisë të prezantuara nga Microsoft në Windows 7. Njëkohësisht, uroj që përmes këtij artikulli të nxis sado pak tek secili nga ju që përdorni sistemet operative te Microsoft në baza ditore që edhe ju të bëni një vlerësim të sinqertë profesionalisht të sigurisë së Windows 7.

Veglërit dhe tiparet e reja në Windows 7

S'ka dyshim se lista e veglërive dhe tipareve të sigurisë të prezantuara në Windows 7 nuk është edhe e pakët! Në vijim do të përmend disa nga to:



Action Center: që të gjithë e dimë që ky është vendi qendrorë që paraqet paralajmërimet dhe ndërmarrim hapat konkret për të siguruar punën e shëndetshme të Windows-it. Edhe pse kam përshtypjen që Action Center nuk është gjë tjetër vetëm se një Security Center i Windows Vista i avancuar, ne fakt është komponenti Maintenance që e bën unik dhe të dallueshëm atë.

Internet Explorer 8: një shfletues i jashtëzakonshëm por mjaftë i përfolur për shpejtësinë dhe sigurinë e tij që më bënë të mendoj sikur Windows 7 nuk duket të jetë shtëpia e tij e vërtetë duke ndikuar kështu në një fare mase edhe në performancën dhe sigurinë e përgjithshme të Windows 7. Së fundi, Microsoft ka prezantuar ca arnime të sigurisë dhe zgjidhje të problemeve në IE 8 që duken të jenë premtuese.

AppLocker: paraqet një hap përpara për të mbajtur të sigurt aplikacionet tuaja. Flitet të jetë i vështirë për t'u përdorur në biznes "*për shkak të ndryshimeve të mëdha që aplikacionet i*

bëjnë dhe faktit që AppLocker nuk përmban aftësinë dinamike". Pavarësisht, kjo duket të jetë më shumë çështje performance se sa sigurie.

Direct Access: kurrë nuk ka qenë më lehtë, më me transparencë dhe të gjitha në një vend për të konfiguruar një lidhje gjithnjë-aktive të sigurt me rrjetin e korporatës suaj. Një produkt i qëlluar, në vend të merituar dhe në kohë të duhur i përkrahur vetëm nga disa versione të Windows 7. Nuk arrije ta kuptoje pse Microsoft nuk e ka përfshirë në versionin e Windows 7 Professional duke e ditur që ky version i dedikohet biznesit gjithashtu?

BranchCache: i bën përdoruesit në distancë të ndjehen sikur punojnë në zyrën kryesore. Një veglëri e jashtëzakonshme për produktivitet të punëve në zyrë me siguri të lartë, por sërish e përkrahur vetëm nga disa versione të Windows 7. Sërish Windows 7 Professional mbetet i përjashtuar!

Homegropup: kurrë nuk ka qenë më e lehtë për përdoruesit shtëpiak që të realizojnë një rrjet kompjuterik shtëpiak. Nga aspekti i sigurisë, më habit fjalëkalimi i … ! Çka, në qoftë se ky fjalëkalim do të piratohet?

Veglërit dhe tiparet e përmirësuara në Windows 7

Përveç veglërive dhe tipareve të reja të prezantuara në Windows 7, në mënyrë shumë të zakonshme edhe Windows 7 përmban veglëri dhe tipare të versioneve të më hershme të Windows-it por të përmirësuara. Disa nga to po i paraqesim në vijim:

ASLR & DEP: apo Address Space Layout Randomization dhe Data Execution Prevention të prezantuar në IE 7 të Windows Vista thuhet të jenë përmirësuar dhe avancuar dukshëm në Windows 7 dhe në IE 8 të tij përfshi këtu edhe mbrojtjen e kernellit të vetë sistemit operativ. Megjithatë, edhe përkundër këtyre avancimeve të dhënat flasin që janë identifikuar lëshime në nivelin e sigurisë së kernellit të cilat mundësojnë qasje të paautorizuar dhe ekzekutim të kodit të keq nga distanca.

BitLocker To Go: paraqet një evoluim të natyrshëm të BitLocker të prezantuar në Windows Vista. Duke qenë se roli kryesor i tij është sigurimi i pajisjeve mobile, atëherë e kam quajtur "një dry mobil".

UAC më i mirë: mendoj që të gjitha kritikat negative që Windows Vista i mori në të kaluarën mund ti atribuohen User Account Control i cili dukshëm është përmirësuar në Windows 7. Sa i çuditshëm duket të jetë fakti që vetëm një përmirësim në ndërfaqen e UAC sikur i ka venitur diskutimet e tij në Windows 7!

Windows Firewall: në Windows 7 është akoma më fleksibil, më i lehtë për përdorim dhe i orientuar në rrjet (home, work dhe public). Një falënderim për përmirësimet e bëra në Windows Firewall i takon edhe përdoruesve të cilët aktualisht Microsoft po i dëgjon me shumë vëmendje.

Windows Update: duke qenë se është pjesë e Action Center në Windows 7 e bënë akoma më të arsyeshëm. Padyshim që këtë herë Windows Update e ka tejkaluar veten e tij, përveç përkujdesjes së tij që të mbajë kompjuterin tuaj më të sigurt, ai përditëson softuerin tuaj dhe merr përsipër shkarkimin e drajverëve në rast se të tillët kanë munguar në kompjuterin tuaj.

Veglërit dhe tiparet e trashëguara në Windows 7

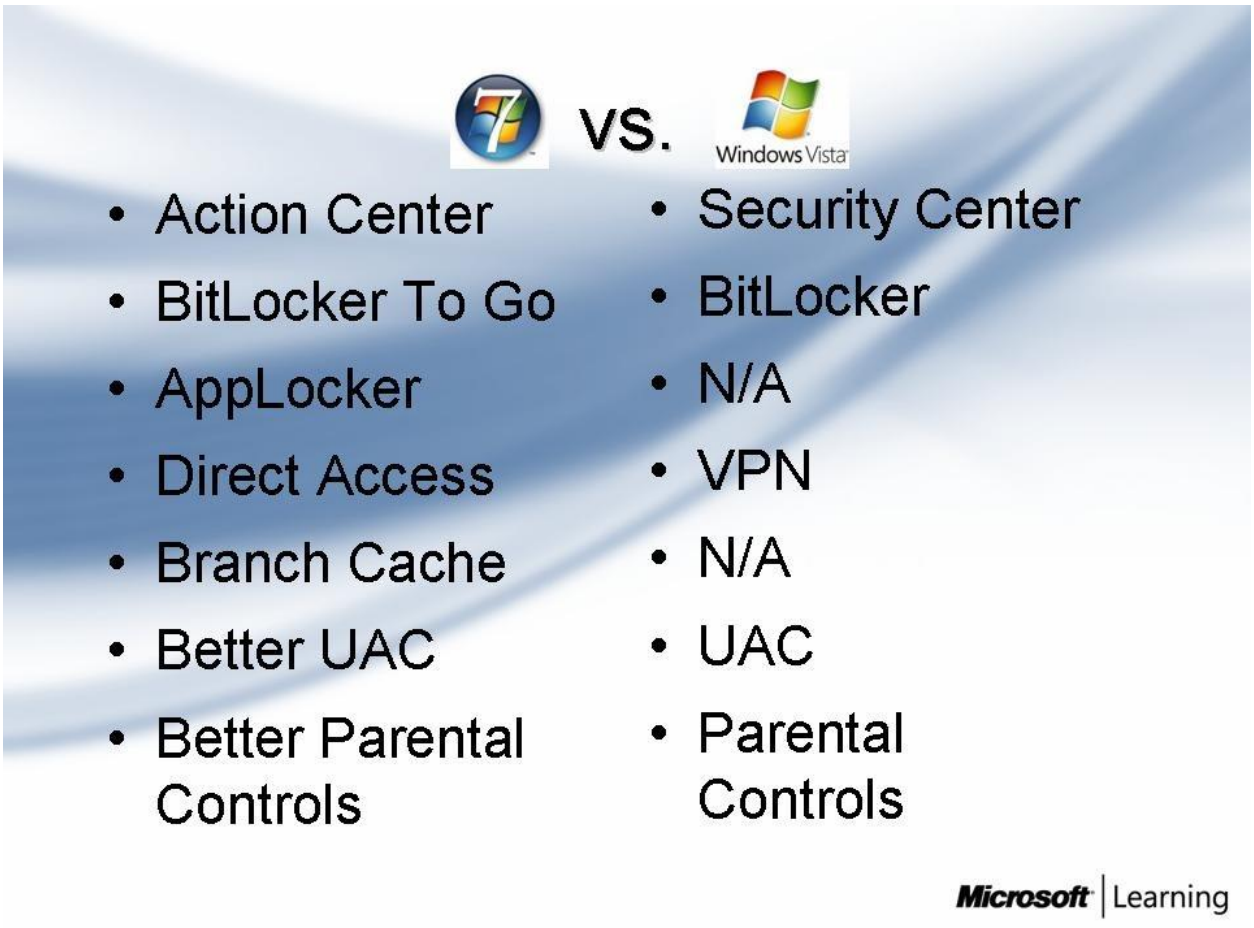
Paksa e çuditshme, por e vërtetë! Edhe Windows 7 përmban veglëri dhe tipare të sigurisë të trashëguara nga versionet e më hershme. Disa nga to janë:

Windows Defender: i dizajnuar ekskluzivisht për ta luftuar spyware-in, u prezantua me këtë emër dhe format në Windows Vista dhe sërish na ofrohet në Windows 7. Një vegël sigurie shumë e mirë, por në Windows 7 sikur ka defekt në servisin e tij që merr përsipër aktivizimin apo çaktivizimin e tij e i cili herë pas here sikur ngatërrohet me vetveten.

Network Access Protection: një vegël rrjeti e jashtëzakonshme e Windows Vista-s e trashëguar në Windows 7 gjithashtu. Natyrisht, ata të cilët më së shumti do lavdërojnë këtë veglëri janë administratorët e rrjetit.

Windows 7 vs. Windows Vista

Duke ditur që platforma Defense-in-Depth në Windows 7 ka origjinë nga Windows Vista, atëherë në shkallë të caktuar mund të themi që siguria në Windows 7 nuk është gjë tjetër veçse siguria e përmirësuar dhe e avancuar e Windows Vista-s, e që ne fund fare të jetë e pranueshme për secilin nga ne. Në vijim le të bëjmë një krahasim të natyrshëm për të parë kush ku qëndron:



Action Center vs. Security Center – të dy veglërit janë për lëvdatë edhe pse për një nuancë më lartë qëndron Action Center falë komponentës Maintenance të përfshirë në të e që në fakt e bënë logjikisht më të organizuar.

BitLocker To Go vs. BitLocker – në mënyrën si ka evoluar kjo veglëri më bën të kuptoj se Microsoft është i mirë në Diplomaci po aq sa është i mirë edhe në Zhvillim.

AppLocker vs. N/A – në sigurimin e aplikacioneve Windows 7 qëndron më lartë se Windows Vista. Megjithatë, vlen të përmendet këtu edhe Application Isolation i prezantuar në Windows Vista.

Direct Access vs. VPN – thuhet që: "*Microsoft e ka ri zbuluar qasjen nga distanca me Direct Access*"!

BranchCache vs. N/A – së bashku me Direct Access duket sikur do ti hapin rrugën teknologjive të reja të rrjetit të cilat priten të prezantohen në Windows 8 kur do të ballafaqohemi me kompjuterët në lëvizje dhe rrjetat në re.

UAC më i mirë vs. UAC – një koncept i jashtëzakonshëm sigurie i prezantuar në Windows Vista i përmirësuar lehtë në Windows 7. A paraqet kjo një përpjekje të Microsoft-it për të lëvizur drejt formatit të sigurisë së llogarive të përdoruesve si edhe Linux? Këtë nuk e di, por koha do ta tregojë!

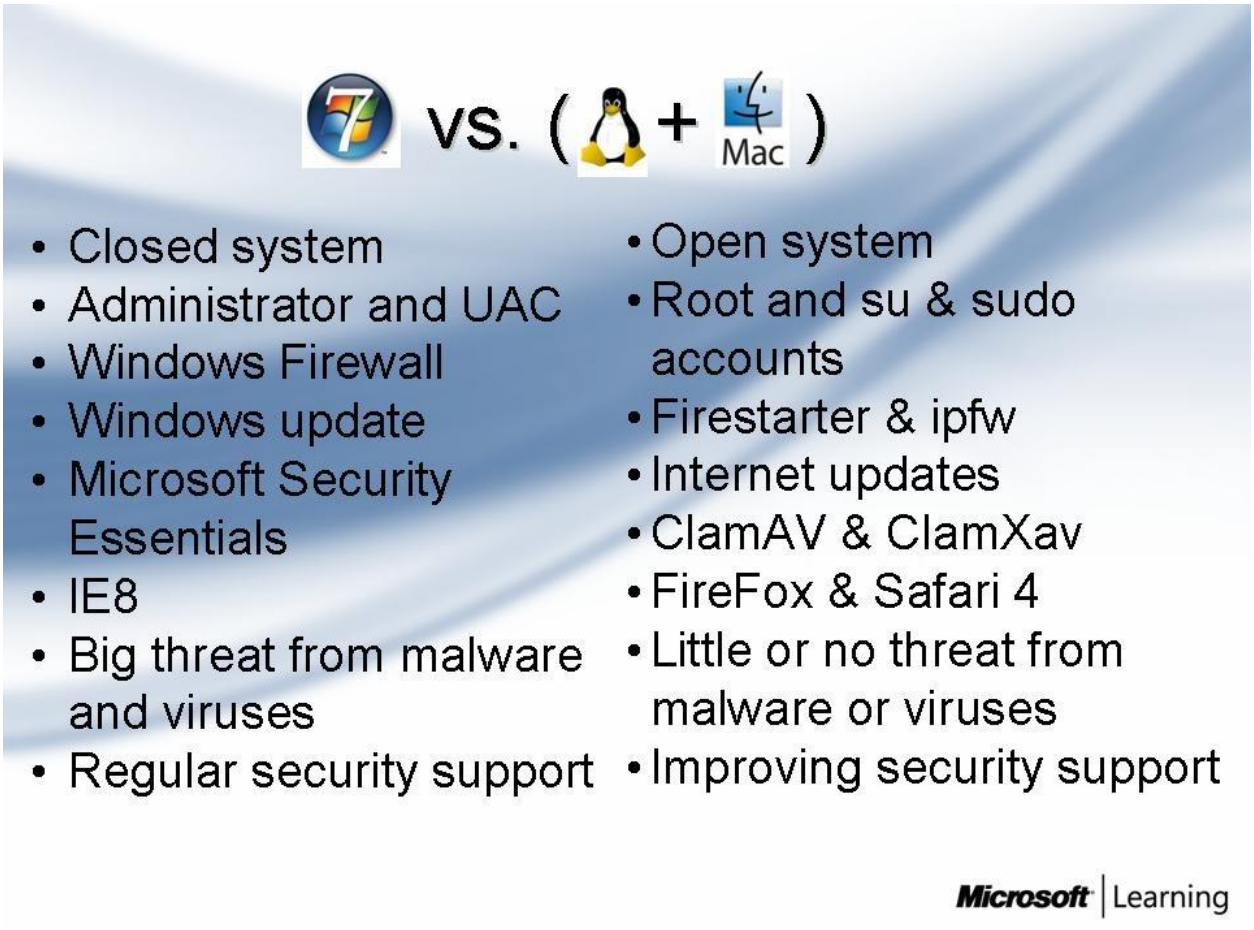
Kontroll Prindëror më i mirë vs. Kontroll Prindëror – sërish një vegël sigurie e jashtëzakonshme e prezantuar në Windows Vista dhe e avancuar në Windows 7. Pyes nëse prindërit tashmë kanë rënë në dashuri me Windows 7?!!!

Është e qartë që shumë veglëri dhe tipare të sigurisë të Windows 7 dhe Windows Vista mbesin për tu krahasuar. Thjeshtë, me këto që u përmendën këtu vetëm desha ta rikujtoj secilin nga ne se cila është zanafilla e vërtetë e sigurisë së Windows 7.

Windows 7 vs. LiMac

Në qoftë se leximi i deri tanishëm ju ka bërë të ndjeheni të fjetur në këtë ditë të nxehtë vere, përmbajtja në vijim do ta ngrit akoma më shumë temperaturën! Fjalët si: cili performon më mirë?, cili është më i sigurt? dhe shumë të këtilla i lexojmë dhe i dëgjojmë pothuajse çdo ditë. Sa për referencë, Marious Oiaga në artikullin e tij: "*Windows vs. Linux vs. Mac"* të datës 24 Mars 2007 ndër të tjera shkruan: "*Gjatë këtij muaji në mënyrë të qëndrueshme është derdhur sasi e madhe e ngjyrës për shkrim për tu krahasuar Windows, Linux dhe Mac OS X*." Përqendroni vëmendjen tek fjala "*këtë muaj*" nga fjalia e cituar! Gjithnjë sipas Oiaga, në Marsin e vitit 2007 duket të jenë bërë shkrime të shumta në mes të profesionistëve të TI-së vetëm e vetëm për të përcaktuar se cili nga sistemet operative është më i mirë nga këndvështrimi i sigurisë dhe performancës. Sido që të jetë në rreshtat në vijim nuk është qëllimi im që të rrisim volumin e këtij lloj diskutimi apo debatimi, përkundrazi ne si përdorues të sistemeve operative të Microsoft-it duam të përcaktojmë vendin e merituar të Windows në mesin e gjithë atyre sistemeve operative që aktualisht ndodhen në treg.

Shënim: kudo që e përmend LiMac, ta dini që po i referohem Linux-it dhe Mac OS së bashku.



Sistemi i mbyllur vs. Sistemi i hapur – më duket sikur ka nga ata përdorues që nuk e donë Windows-in vetëm pse është sistem i mbyllur! Përderisa LiMac është sistem i hapur, në anën tjetër Microsoft-i në një farë mënyre përmes Shared Source Initiative të saj po mundohet të krijojë sado pak një balancë në treg. Sido që të jetë situata aktuale, koha do të tregojë nëse një ditë në të ardhmen Windows do të jetë sistem operativ tërësisht i hapur.

Administratori dhe UAC vs. Root dhe su & sudo – siç e dimë në Windows qëndron Administratori në maje të piramidës së privilegjeve të përdoruesve, ndërsa në LiMac është Root super përdoruesi që administron sistemin në tërësi. Megjithatë, praktika na dëshmon që Administratori nuk ndodhet në maje të piramidës së privilegjeve në Windows meqë disa shërbime menaxhohen nga përdoruesi Local System i Windows NT, për dallim në LiMac nuk ka

përdorues me privilegje më të larta se Root. Mu për këtë arsye, në pjesën që po bëja krahasimin e sigurisë së Windows 7 me Windows Vista, kur po flisja për UAC bëra pyetjen në mos vallë Microsoft po ecën drejt qasjes së Linux kur kemi të bëjmë me përdoruesin për administrimin e tërësishëm të sistemit operativ?!!!

Windows Firewall vs. Firestarter dhe ipfw – është interesant fakti që Windows Firewall në një masë të caktuar lavdërohet edhe nga përdoruesit e LiMac.

Windows Update vs. Internet Update – edhe përkundër avancimeve të shtuara në botën LiMac kur kemi të bëjmë me përditësimet e sistemit operativ, duhet ta pranojmë faktin që në këtë segment Windows 7 fiton betejën. Windows Update është më i kompletuar, proaktiv dhe më i përshtatshëm për përdorim.

Microsoft Security Essentials vs ClamAV dhe ClamXav – edhe përkundër softuerëve AntiVirus të rekomanduar, në të dy platformat si atë Windows ashtu edhe në LiMac përdoruesit janë tërësisht të lirë të instalojnë softuerin e dëshiruar. Duke pas për bazë faktin që MSE është produkt i Microsoft-it dhe është Microsoft ai që njeh më së miri kodin burimor të sistemeve të tija operative; dhe faktit tjetër që MSE së fundit është pozicionuar në mesin e softuerëve AntiVirus më të njohur në botë, atëherë s'ka dyshim që Windows sërish në këtë segment qëndron më lartë se LiMac.

IE 8 vs. Firefox dhe Safari 4 – që të tre këta shfletues kanë probleme të caktuara. Sipas përfaqësimit në treg është IE 8 ai që udhëheqë bindshëm, ndërsa sipas testeve Benchmark është Firefox që prinë garën e shfletuesve. Një gjë është më se e vërtetë: Microsoft po punon në versionin e ri të shfletuesit të tij IE 9, të njëjtën po bëjnë Mozilla Foundation me Firefox-in e tij dhe Apple me Safarin e tij.

Kërcënim i lartë nga kodi i keq dhe viruset vs. Pak ose aspak kërcënim nga kodi i keq dhe viruset – duhet ta pranojmë faktin që Windows në të kaluarën ka pasur probleme serioze me sigurinë, të cilat në mënyrë lineare kanë filluar të ulen që nga Win2k. Mbase kjo situatë e ka bërë që të jetë sistemi operativ më i kërcënuar nga kodi i keq dhe viruset, njëkohësisht duke e pozicionuar në pozitën e parë si sistemi më i përfolur në botën e sigurisë. Mbase gaboj në vlerësimet e mia, por kam përshtypjen se po tu ndërrojmë vendet Windows-it dhe LiMac-ut në treg, gjithsesi do të kishim një situatë tjetër. Ky supozim mbetet vetëm se

hipotezë, ndërsa realiteti flet që Microsoft është në rrugë të mirë të ofrojë një sistem operativ nëse jo të përkryer atëherë të sigurt gjithsesi.

Përkrahje e vazhdueshme e sigurisë vs. Përkrahje e përmirësuar e sigurisë – mendoj se merita i përket faktit që Windows është sistem i mbyllur.

Windows 7 dhe e ardhmja e tij

Duke pas parasysh të gjitha veglërit dhe tiparet e sigurisë që u përmendën në këtë artikull si dhe shumë të tjera që nuk janë përmend e të cilat janë pjesë përbërëse e sigurisë të Windows 7, vetvetiu lind pyetja: A është e mjaftueshme kjo siguri? Deri sa ne përpiqemi ti përgjigjemi pyetjes së parashtruar, kujtojmë faktin se Microsoft po punon në zhvillimin e sistemit operativ të ri Windows 10 që sipas informatave nga Interneti pritet të paraqitet në treg diku kah mesi i vitit 2015.

Konkluzioni

Edhe pse Windows (përfshi këtu edhe Windows 7) është sistemi operativ më i përdorur në botë në kompjuterët personal, vazhdon të jetë i cenueshëm nga aspekti i sigurisë edhe pse me Windows 7 është ulur dukshëm shkalla e kërcënimeve nga kodi i keq dhe viruset. Pavarësisht nga të gjitha këto, po ti peshojmë anët pozitive që Windows 7 ofron në rrafshin e sigurisë me ato negative që prekin karakterin e Windows 7, mbase për herë të parë në historinë sistemeve operative të Microsoft të dedikuar për kompjuterët personal, do të vërejmë që ana pozitive e peshores ka filluar të merr anën. Me këtë mund të themi që nëse Microsoft me Windows 7 nuk ka ofruar një sistem operativ me siguri të përkryer, atëherë ka ofruar një që është shumë i sigurt. Kështu, siguria e Windows 7 mund të shërbejë si platformë e mirë që Microsoft në një të ardhme të afërt të zhvilloj një sistem operativ me siguri të përkryer, mbase Windows 10!

Shtojca B: Arkivimi i të dhënave në Internet

"Në qoftë se njerëzit nuk i japin komplement njëri tjetrit, atëherë aty do të ketë shoqëri të vogël." Luc de Clapiers

Siguria fizike është term që përdoret për të përshkruar sigurinë që ofrohet jashtë sistemit kompjuterik dhe të rrjetit. Zakonisht, komponentët e rëndomta të sigurisë fizike që frenojnë sulmet direkte janë: rojet e sigurimit, drynat, thurjet, dhe kamerat e vëzhgimit. Shumica e masave të sigurisë fizike janë rezultat i arsyes së përbashkët e të menduarit dhe planifikimit dhe si të tilla shpesh janë zgjidhje evidente. Kështu, të gjitha përpjekjet për të siguruar kompjuterët, serverët dhe resurset e rrjeteve do të jenë të pakuptimta në qoftë se impianti fizik që i strehon ata nuk është i mbrojtur.

Sot, në mesin e gjithë atyre kompanive që ofrojnë produkte nga më të ndryshmet për ruajtjen fizike të të dhënave është edhe Iron Mountain, kompani e specializuar për ruajtjen dhe restaurimin e të dhënave. Ndër produktet e shumta të Iron Mountain është edhe shërbimi PC Backup/Server Backup i cili ofron siguri në çdo nivel që nga rezervimi i të dhënave e deri te rinxjerrja e tyre. Në rreshtat në vijim do të shpalosen veçoritë e këtij produkti me theks të veçantë në masat e sigurisë që ndërmerr Iron Mountain që të garantoj se të dhënat e klientit janë të sigurta nga qasjet e paautorizuara fizike dhe përmes Internetit, apo se edhe janë të sigurta edhe nga qasjet e vetë nëpunësve të kompanisë Iron Mountain.

Çka është shërbimi PC Backup/Server Backup?

Shërbimi PC Backup/Server Backup paraqet një zgjidhje që bazohet në arkitekturën klient/server ashtu që të rezervoj të dhënat nga secili kompjuter kudo në botë me anë të çdo rrjeti TCP/IP në dispozicion. Serveri tufëz qendror përdoret për ruajtjen e të dhënave të rezervuara, e i cili server mund të jetë në lokalitetin e Iron Mountain ose në lokalitetin e partnerit. Në të dyja rastet menaxhohet nga Iron Mountain

Rezervimin e të dhënave e bën Connected Backup/PC Agent i cili është një aplikacion i vogël që instalohet dhe ekzekutohet në njërin nga kompjuterët e korporatës, biznesit apo organizatës. Connected Backup/PC Agent është më shumë se një vegël për rezervim të të

dhënave, meqë kujdeset edhe për planifikimin e rezervimit, mundësimin e rinxjerrjes dhe gjenerimin e evidencave te nevojshme nga transaksionet e këtyre aktiviteteve të rezervimit të të dhënave. Edhe pse rezervimi i të dhënave i realizuar përmes rrjetit kërkon më shumë brez të komunikimit, teknologjia e patentuar për reduktim të të dhënave përkujdeset që të kompleton shume shpejtë edhe rezervimin e të dhënave në sasi të mëdha. Ky softuer është i aftë që të ofron rezervimin dhe restaurimin e të dhënave edhe në shpejtësitë e komunikimit të rangut të lidhjes telefonike 28.8 kbps.

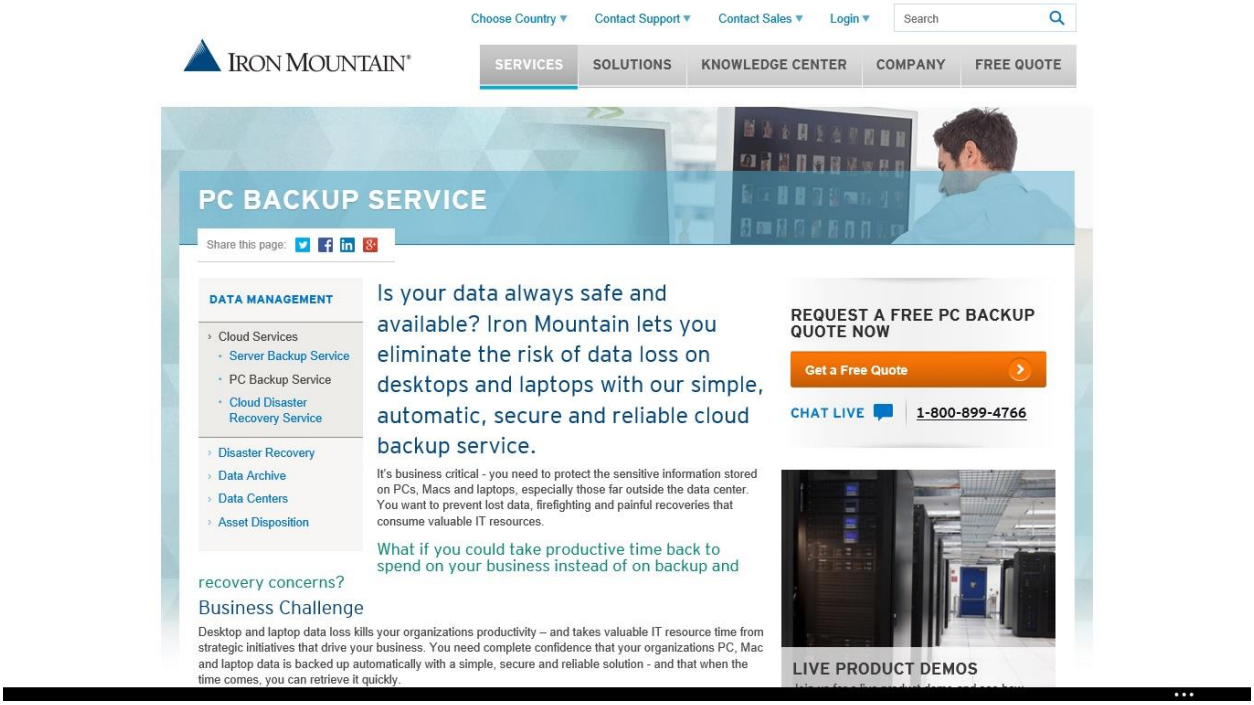


Figura 1: Shërbimi PC Backup

Siguria në shërbimin PC Backup/Server Backup

Ashtu siç u përmend në rreshtat paraprakë, shërbimi PC Backup/Server Backup është zgjidhje që bazohet në arkitekturën klient/server ku në anën e klientit ekzekutohet aplikacioni Connected Backup/PC Agent që inicion rezervimin e të dhënave, ndërsa në anën e Qendrës së të Dhënave ndodhet tufa e serverëve qendror me përgjegjësi të magazinimit, mbrojtjes, dhe menaxhimit të të dhënave që vijnë përmes procesit të rezervimit. Me qëllim të garantimit të sigurisë në një mjedis të rrjetit kaq kompleks ofrohen rregullatorët e sigurisë si në vijim:

- **Sesioni i Sigurt i Rezervimit dhe Rinxjerrjes:** është Connected Backup/PC Agent ai i cili ekzekuton rezervimin dhe rinxjerrjen e të dhënave në anën e klientit. Agjenti në rezervimin e planifikuar e ekzaminon diskun e klientit për të përcaktuar se cilat të dhëna duhet dërguar për magazinim. Përmes TCP/IP socket agjenti kontakton Qendrën e të Dhënave dhe me anë të teknologjisë SSL të dhënat transmetohen në formë të sigurt. Serveri tufëz qendror e autentikon agjentin me anë të çelësit të tij, ndërsa agjenti e autentikon serverin përmes certifikatës. Agjenti përdorë çelësin AES 128 bit për të enkriptuar dhe nisur transmetimin. Ne skajin tjetër serveri tufëz qendror i paketon në një skedarë të vetëm të gjithë skedarët e enkriptuar të pranuar dhe të njëjtin e arkivon në format të enkriptuar. Kur të vjen koha e rinxjerrjes, agjenti e kontakton serverin tufëz qendror dhe të njëjtit i dërgon listën e skedarëve që duhet rinxjerr. Serveri tufëz qendror i transmeton skedarët e enkriptuar deri tek klienti, me çka pastaj skedarët e pranuar do të deshifron nga agjenti dhe të njëjtit do të vendosen ne diskun e klientit. Klienti përdorë fjalëkalimin për autentikim përpara se të fillon procesi i rinxjerrjes. Si rezultat i qasjes fizike ne kompjuterin e klientit pamundësohet rinxjerrja e të dhënave nga personat e paautorizuar.
- **Siguria e Arkivimit:** në serverin tufëz qendror të dhënat enkriptohen me algoritmin e çelësit AES 128-bit dhe të njëjtat arkivohen në formatin e njëjtë. Serveri tufëz qendror në lokalitetin e Iron Mountain shërben si depo për ruajtjen e të dhënave dhe nuk është pjesë e infrastrukturës të sistemit për komunikim. Kjo është bërë me qëllim që të parandalohet leximi i të dhënave në rast se individi arrin të realizoj qasje të paautorizuar deri tek të dhënat.

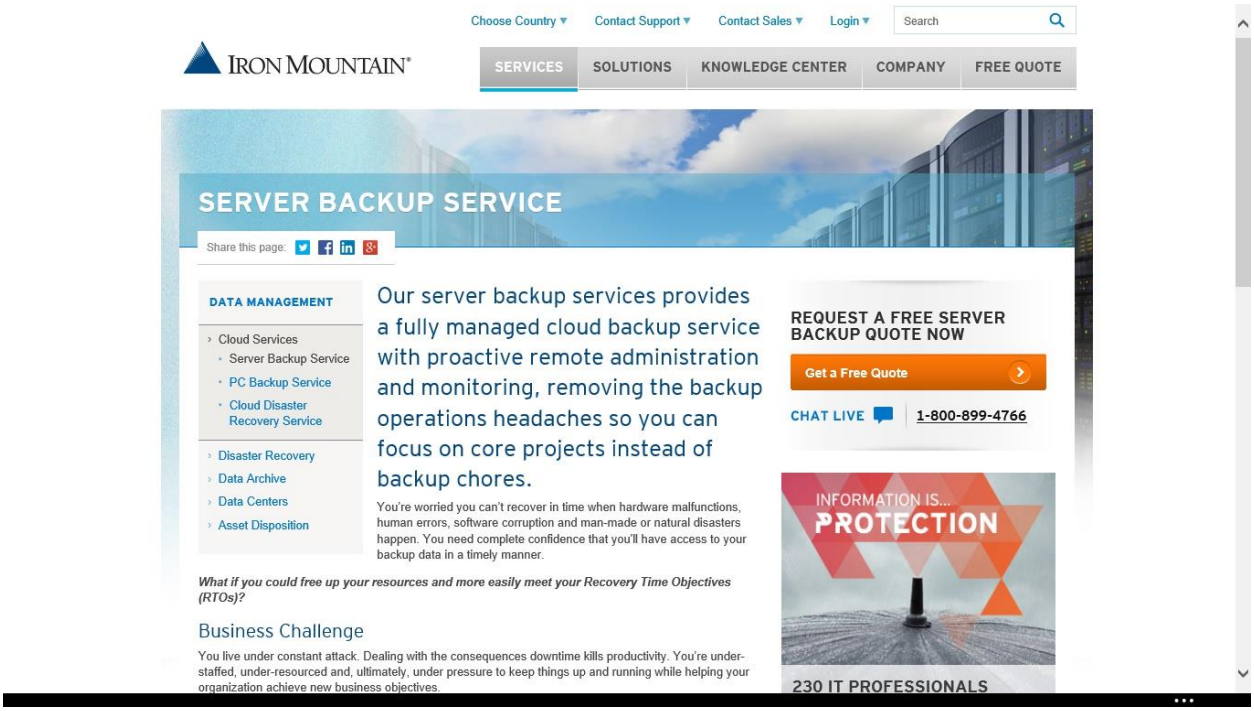


Figura 2: Shërbimi Server Backup

- **Siguria e Rrjetit dhe Murit mbrojtës:** të gjitha të dhënat e rezervuara të pranuara nga serveri tufëz qendror dyfishohen në lokalitetin pasqyrë që ndodhet në lokalitet anonim. Politikat e sigurisë të murit mbrojtës nuk lejojnë qasje direkte nga jashtë në të dhënat që ruhen në serverin tufëz qendror. Port i caktuar përdoret për trafikun e jashtëm. Gjithashtu pjesë e sistemit të sigurisë së rrjetit janë edhe sistemet për detektim të ndërhyrjes. Zakonisht mbahen 10 versionet e skedarit të ruajtur, ndërsa skedarët e fshirë mbahen deri në 90 ditë. Në protokollin e komunikimit në mes të klientit dhe serverit nuk ka asnjë komandë që lejon fshirjen e skedarëve.
- **Siguria e Llogarisë së Përdoruesit:** me qëllim që të bëhet përshtatje konform kërkesave të klientit, atëherë secili instalim i PC Backup/Server Backup është unik për secilin klient. Administratori posedon të drejtën që të përshtat rregullat administrative dhe rinxjerrjen e llogarive të përdoruesve. Për restaurimin të llogarive të përdoruesve nevojitet çelësi i enkriptimit. Gjithashtu përdoret edhe LDAP për rinxjerrjen e të dhënave që janë të mbrojtura me fjalëkalim. Kjo mundësohet me anë të Enterprise Directory Interface. Tiketa që ofrohet me anë të postës elektronike e që e shoqëron procesin e instalimit te agjentit, përmban shifrën për regjistrim të njëhershëm në server. Për të

garantuar që përdoruesi qas vetëm skedarët e tij apo skedarët e ndërlidhur për llogarinë e tij, përdoret File Security Descriptor i cili konfigurohet në nivel dosje apo skedari në kompjuterin e klientit.

Konkluzioni

Sot kur përdorimi i Internetit për të bërë biznes ndodhet në nivelin më të lartë të historisë së tij, atëherë s'ka dyshim se ndër sfidat kryesore te biznesit të shekullit 21 mbetet edhe arkivimi i sigurt i të dhënave. Ky aktivitet bëhet akoma më i ndërlikuar dhe i pa arritshëm për një numër të madh biznesesh që nuk posedojnë ekspertizën dhe paratë e duhura. Mbase për këto biznese opsion i mundshëm mund të jenë shërbimet e Iron Mountain me theks të veçantë shërbimi PC Backup/Server Backup. Ky shërbim në mënyrë virtuale eliminon rizikun e humbjes së të dhënave në kompjuter duke kryer në mënyrë automatike rezervimin e të dhënave përderisa përdoruesit merren me aktivitetet e punëve të tyre të përditshme.

Faleminderit!

Faleminderit për kohën dhe konsideratën tuaj për të lexuar e-Librin tim! Në qoftë se ju ka pëlqyer ky e-Libër dhe dëshironi të merrni pjesë aktive në përmirësimin e mëtutjeshëm të këtij e-Libri, atëherë dërgoni:

- propozimet
- sugjerimet dhe
- vërejtjet tuaja

në e-Postën BekimDauti@BekimDauti.com. Me shumë kënaqësi do ti lexoj dhe do të përpiqem ti përfshijë në ribotimet e radhës.