UDHEZUES PER SIGURINE NE INTERNET DHE SHMANGIEN E RISKUT

Karta e Elementeve te Sigurise (Rregulla sigurie)

Teknologjia e informacionit dhe interneti perbejne nje potencial te madh per administraten, bizneset e industrise dhe qytetareve. Ne te njejten kohe, mundesite e reja teknike sjellin me vete edhe kercenime.

Ne vitet e fundit, ne nje shkalle te papare ndodhin edhe variantet e malvere qe kercenojne IT sistemet e sigurise. Gjithashtu, krahas sasise ne rritje, kemi parasysh edhe nje cilesi te ndryshimit te kujdesit. Programet Malicious sot nuk jane ato qe ne mase te gjere shkaktojne deme te drejtperdrejta dhe te perceptueshme, por kontrollin mbi kompjuterin per te siguruar ne periudha te dhena te zgjeruara per spiunazh. Rrezik per konsumatoret dhe bizneset jane viktimat e spiunazhit te cilet jane ne shenjester te sulmeve.

Siguria e atdheut ne shoqeri moderne do te thote siguri te informacionit dhe te sigurise se informacionit te nderlikuar dhe infrastruktura e komunikacionit. Besimi ne sigurine dhe besueshmerine e informacionit dhe teknologjive te komunikimit qe eshte edhe thelbesor nese ne jemi ne gjendje per te shfrytezuar mundesite e shoqerise se informacionit. Ruajtjen afat-gjate, dhe besimi ne shperndarje te informacionit eshte detyre prioritare,dhe me kete duhet te merret Ministrise Puneve te Brendshme.

Te arriturat e zhvillimit teknik ne mase te gjere dhe zhvillimi i Internetit, me kohe do te behet nje “infrastrukture kritike” per vendin dhe biznesin, sepse infrastruktura Internet eshte nje pike nevralgjike e çdo organizate politike dhe ekonomike. Avantazhet e IT sistemeve funksionale mund te perdoren vetem nese siguria eshte e organizuar plotesisht. Prandaj, çdo shtet duhet te shikoje kete si nje detyre te rendesishme.

Udhezues per mbrojtjen e rrjetit dhe kompjuterit

Penetrimi ne rritje te biznesit dhe botes se perditshme me teknologjine e informacionit kerkon mbrojtje te gjere ne perdorimin e teknologjise se informacionit. Per kompanite, mjetet e lidhjes se rrjetit te internetit jane veçanerisht te rrezikuara. Nje porte e sigurise siguron nje mbrojtje te mundur per nje shtepi. Operimi i sigurt i kompjuterit dhe rrjetit eshte e mundur vetem nepermjet kombinimit te masave te mbrojtjes teknike dhe sjellja e pergjegjesise e te gjithe te punesuave.

Teknologjia e informacionit eshte bere nje pjese perberese e administrates, biznesit dhe shtepise.

Siguria, gjithashtu mbeshtetet ne sistemet elektronike dhe harduer&softuer aplikacione te shumta. Users, nga shtepia korrin perfitimet bankare online, ose online per te blere produkte permes internet. Prandaj, paraprkisht duhet te merren masa te pershtatshme te sigurise per te parandaluar deme te mundshme.

Çdo kompjuter, qofte ne nje shtepi private, ne nje kompani apo nje autoritet, potencialisht eshte i rrezikuar. Numri i madh i programeve me qellim te keq vjen me e-mail ne kompjuterin tuaj. Nje infeksion i kompjuterit permes mediave te tilla si DVD ose USB eshte gjithashtu e mundur. Nderkohe, vizita ne web faqe eshte e mjaftueshme per te manipuluar dikush tju infektoje PC-ne.

Ndodh qe, te jemi te infektuar dhe kompjutri na mundeson te jete ne gjendje per te lexuar te dhenat, te ndryshohen ose fshihen. Megjithate, nese nuk jane masat mbrojtese te mjafstueshme, rreziku i infeksionit nuk mund te reduktohet nga programet keqdashese. Per mbrojtjen baze te nje PC-e, nje program antivirus rregullisht i perditesuar eshte kusht per sigurimin e sistemit operativ dhe aplikacione te tjera.

Rrjetet lokale dhe publike:

Ne pergjithesi, sot sistemet IT jane te lidhura me rrjetet lokale dhe operues publik. Ne veçanti, lidhje te internetit per perpunimin e informacionit luan nje rol gjithnje e me te rendesishem. Kjo mund te jete permes lidhjeve te internetit te drejtperdrejte, pasi ato i gjejme shpesh ne ekonomi, lidhje familjare private, ose nepermjet nje rrjeti lokal. Lidhje te rrjeteve publike, gjithashtu sjellin nje shumellojshmeri te rreziqeve qe lidhen me te dhe nevojen per te marre masat e duhura mbrojtese. Ne praktike disa kompjuter kane te ashtu-quajtur firewall personal me vlere. Por, nese nje rrjet lokal ku ju mund te gjeni disa lidhje IT te lidhura me nje rrjet publik, kjo duhet te jete i mbrojtur nga aksesi i paautorizuar. Per kete, nje porte e sigurimit (firewall) midis rrjetit lokal dhe rrjetit publik duhet te vihen ne veprim, i cili do ushtroje kontrollon e kerkesave hyrese dhe dalese.

Personeli, infrastruktura dhe çeshtje organizative:

Informacionet e paraqitura jane vetem shembuj te masave te sigurise, qe kane deshmuar si te suksesshme, dhe qe gjenden edhe sot. Perveç kesaj, ne nje sere te aspekteve te tjera, gjithmon duhet te jene ne dukje, konfigurimi i sigurt, backups, dhe hyrje kriptimi. Perveç kesaj, duhen gjithashtu aspektet njerezore, infrastrukturore dhe organizative. Pa rregulla te qarta mbi perdorimin e Internetit dhe trajnimin e stafit administrativ, pa nje internet Siguri te qendrueshme, asnje ndermarrje apo individ nuk do te jete i mbrojtur. I rendisim me poshte:

Siguria e informacionit dhe te dhenave:

Sigurine e informacionit dhe te dhenave duhet shikuar si nje qasje sekrete per kete arsye duhet te kuptohet brenda kompanise dhe zbatohet ne perputhje me rrethanat. Veçanerisht te pershtatshme per kete qellim jane te ashtuquajtura Informacione te Menaxhimit te Sistemit te Sigurimit. Kjo do te ndihmoje per te percaktuar sigurimin e informacionit te perhershme, per te kontrolluar dhe per te permiresuar vazhdimisht. Nese te gjitha masat e standardit te sigurise zbatohen ne mbrojtje te IT, mundesit jane te medha qe kjo te konfirmoje me nje çertifikate ne perputhje me "ISO 27.001 ne baze te mbrojtjes IT ".

Njohja dhe bashkepunimi me ALCIRT:

Perveç keshillave mbi sigurine, ALCIRT eshte institucioni kryesor qe mbikqyr dhe harton rregulla per sigurine e rrjeteve IT. ALCIRT jep informacione te thella me publikime te ndryshme te cilat i gjejme edhe ne internet faqe te ALCIRT ne dispozicion. Me informacione te ALCIRT ne dispozicion te qytetareve eshte shpjeguar per te kuptuar, se çfare te marrin ne konsiderate perdoruesit privat te IT, dhe IT sigurise konkrete. Ju mund te vizitoni faqen e internetit te ketij institucioni www.cyberalbania.al.

Çeshtje te rendesishme jane ketu, per shembull, per perdorimin e sigurt te Internetit, viruset dhe demtues te tjera, si dhe keshilla per rrjete pa tela (WLAN). Detaje ne te gjitha aspektet e IT-sigurise mund te gjenden ne faqen e internetit te ALCIRT. Autoritetet dhe kompanite mund te gjejne atje rregulla dhe keshilla te ofruara nga ALCIRT rreth temes te IT-sigurise.

Kohet e fundit Microsoft njoftoi nje dobesi te re ne Internet Explorer. Edhe nje sulmues i dobet mund te lexoje informacione nga pjesa lokale e nje sistemi te prekur. Dobesia eshte zbulimi ne te gjithe versionet e Internet Explorer me sistemet operative Windows. Per shkak te menyres se re te mbrojtjes ne sistemet e reja operative Windows dhe versionet e Windows Internet Explorer 11, nuk jane prekur. Se paku, nese ata jane te operuar ne konfigurimin baze te sigurt, me shfletuesin e sistemeve operative te fundit Microsoft. Microsoft gjithashtu jep qartesi per sistemet operative Windows 2008 dhe Windows 2013.

Windows 10 eshte aktualisht ne progres dhe ka arritur mbi 800 milion instalime deri sot. Eshte e rekomanduar per perdoruesit e ketyre sistemeve operative perkohesisht te kalojne ne nje alternative web browser Chrome, Mozilla, etj qe ne kohet e sotme jane shume mire te mbrojtura.

Surfim/navigim i sigurte:

Sot ka nje numer shume te madh perdoruesish Internet, dhe sipas statistikave me te reja shifra i perdoruesve Internet eshte rreth 2.5 miliard, qe do te thote se se çdo i katerti banore i rruzullit toksore perdore Internet. Per fat te keq, nje perqindje e madhe e ketyre perdoruesve nuk kane njohuri mbi pikat themelore te praktikave te sigurise kur perdorin Internet sherbimet.

Kjo situate per fat te keq krijon nje game te gjere problemesh, duke perfshire infektimin e kompjutereve, vjedhjen e informacionit te fshehte, vjedhjet e identitetit, etj. Ne kete tekst u jepet perdoruesve nje pasqyre e komponenteve te sigurise dhe keshilla per perdorimin e sherbimeve ne internet, per te shmangur befasi dhe siklete, dhe per te u thene si Interneti te perdoret ne menyre efektive dhe te sigurt.

Menyrat per te mbrojtur kompjuterin e klientit:

Hapi i pare ne arritjen e nje perdorimi te sigurt te internetit eshte mbrojtja e kompjuterave personal. Per te qene mbrojtja e kompjuterave personal e plote dhe e sigurt, eshte e nevojshme te siguroni masat adekuate per te garantuar sigurine mbi te gjitha elementet e sistemit kompjuterik.

Elementi i pare qe duhet te merret parasysh eshte sistemi operativ i kompjuterit. Sistemi Operativ (OS) eshte pergjegjes per menaxhimin e burimeve harduer dhe proceset e menaxhimit (aplikacionet) ne kompjuterin tuaj. Sisteme me te popullarizuar qe operojne ne sisteme me te jane versione te ndryshme te Windows, Linux shperndarje te ndryshme, Mac OS X, sistemi operativ Unix, etj Siguria e kompleksitetit operativ mund te arrihet vetem duke aplikuar shtese rregulla te reja dhe te permiresuara te qendrueshme te versionit te fundit.

Ketu duhet te kemi parasysh qe sistemet operative komerciale jane problematike per ti arrnuar me aplikime shtese rregullash dhe rifreskim, nese sistemi operativ eshte blere ne menyre te paligjshme. Ne kete menyre, kompjuteret me sisteme operative te vjeteruar jane ve ne deshtimin e sigurise edhe kur jane riparuar me arna te fresketa.

Elementi tjeter per te mbrojtur kompjuterin tuaj eshte firewall (firewall Ang.). Nje firewall eshte nje program kompjuterik qe sherben per te mbrojtur kunder qasjes se paautorizuar ne kompjuterin e kontrollit te autorizuar te aksesit. Firewall, ne baze te kontrollit te trafikut te rrjetit dhe te rregullave, ka per detyre te pranoje ose refuzoje pakot e informacioneve.

Qe proceset ne kompjutera te ndryshem te komunikojne mes tyre, ato kane nevoje per identifikues (US porte, porte), e cila mund te transmetoje dhe te marre te dhena. Çdo proces ne kompjuter qe do te komunikojne ne nje rrjet (te marre ose per te derguar mesazhe) duhet te perdore nje porte per te arritur komunikim. Sipas parametrave automatike, shume porta ne kompjuterin e perdoruesit jane te hapura. Qe perdoruesi te mund te mbrohet, eshte e nevojshme per te lene te hapur vetem ato porta qe jane te nevojshem per komunikim.

Nje firewall eshte nje program qe lejon perdoruesit ne menyre intuitive per te i ndihmuar ato per te hapur vetem ato portet qe u duhen,dhe mbyllje te porteve te panevojshme duke reduktuar keshtu mundesine e sulmeve te suksesshme ne kompjuter. Firewall me te njohur dhe falas jane ZoneAlarm, firewall Comodo (te cilat mund te shkarkohen individualisht ose si pjese e nje zgjidhje Comodo Internet Sigurimi te

pergjithshme), Online Armor pa pagese, PC Tools Firewall Plus, Outpost Firewall, Windows Firewall i cili vjen ne pako se bashku me Windows.

I fundit ne nje sere te elementeve per mbrojtjen e kompjutereve personal, eshte instalimi i nje antivirus softuer ne PC-ne tuaj. Antivirusi sherben per te kryer zbulimin e viruseve ne kompjuter tashme te infektuar, dhe me masa ne parandalimin e infektimit duke i krahasuar permbajtjet e kompjuterit me ato te marre nga mostrat e viruseve te njohur. Programet Antivirus dallohen nga menyra e dedektimit te viruseve ne rrugen e zbulimit dhe te madhesise se bazes se te dhenave te mostrave te viruseve te njohur.

Nuk ka zgjidhje me te mire per mbrojtje nga viruset, por ka disa zgjidhje cilesore pa pagese per perdorim individual ne shtepi. Me te njohurit antivirus programe te lire (pa pagese) jane Avast, Avira, dhe AVG . Perveç ketyre, duhet te pranojme dhe te permendim edhe Produkte Comodo Internet Security, Avira, AVG, Microsoft Security Essentials, etj te cilet kryesisht ofrojne Siguri dhe zgjidhje te plote (antivirus, antispyware dhe firewall) dhe jane gjithashtu te lire ose pa pagese. Pra eshte e nevojshme eshte qe kompjuteri te kete nje program antivirus dhe nje firewall aktiv.

Megjithate stafi i kompanise tone eshte i gatshem tju asistoje dhe ndihmoje per te zgjidhur ceshtje te sigurise dhe eleminuar nderhyrjete demshme, te paligjshme ne pajisjet e klientit.