Shadow IT

Menaxhimi i 'aseteve të panjohura' që përdoren brenda një organizate

Udhëzimi është përshtatur nga NCSC.GOV.UK
dhe
është i përshtatshëm për Bizneset e vogla e të mesme, Organizatat e mëdha, Sektorin publik

ÇFARË ËSHTË SHADOW IT

Termi "Shadow IT" (i njohur gjithashtu si "IT gri") i referohet aseteve të panjohura që përdoren brenda një organizate.
Meqenëse këto asete nuk konsiderohen gjatë procesit të menaxhimit të aseteve dhe nuk përputhen me proceset ose politikën e IT-së, ato janë një rrezik për organizatën tuaj. Kjo mund të rezultojë në eksfiltrimin e të dhënave sensitive, ose përhapjen e malware në të gjithë organizatën.

Shadow IT zbatohet gjithashtu për teknologjitë Cloud. Për shembull, nëse përdoruesit po ruajnë të dhëna të ndjeshme të organizatës në llogaritë e tyre personale në cloud (me qëllim që t'i aksesojnë ato nga një vendndodhje ose pajisje tjetër), kjo është gjithashtu shadow IT, sepse ruajtja në llogaritë personale të Cloud ndoshta nuk mbulohet nga procesi i menaxhimit të riskut të organizatës suaj.

Shumica e organizatave kanë elementë të Shadow IT, por nëse Shadow IT prevalon mbi asetet e tjera, menaxhimi i riskut bëhet më i vështirë sepse nuk do të keni një kuptim të plotë të aseteve që duhet të mbroni dhe vlerësoni më shumë.

SHADOW IT NUK ËSHTË BYOD

Shadow IT rrallëherë mund të jetë rezultat i qëllimeve keqdashëse. Zakonisht është për shkak të vështirësive të punonjësve për të përdorur mjete ose procese të sanksionuara për të përfunduar një detyrë specifike, duke rezultuar në përdorimin e shërbimeve të pamiratuara zyrtarisht, të cilat i ndihmojnë të përfundojnë punën e tyre.

Disa arsye të zakonshme që çojnë në nevojën e Shadow IT janë:

- nuk ka hapësirë të mjaftueshme ruajtjeje
- pamundësia për të ndarë të dhënat me një palë të tretë
- nuk ka akses në shërbime të caktuara të nevojshme
- nuk ka një aplikacion të miratuar për komunikimet e video-konferencave
- pamundësia për të kërkuar asete ose shërbime përmes rregulloreve të organizatës (ose procesi për të bërë këtë kërkesë është joefektiv /i ngadalshëm)
- aplikacionet e miratuara ose shërbimet SaaS nuk ofrojnë funksionalitetin e kërkuar
- mos kuptimi i rrezikut që mund të sjellë përdorimi i pajisjeve personale ose shërbimeve SaaS

Me një politikë efektive BYOD, organizata ka nën administrim dhe nën kontroll të dhënat e saj dhe burimeve të lejuara në pajisjet e përdoruesve, duke lejuar administrimin e rrezikut. Ky nuk konsiderohet Shadow IT.

Në rastin e Shadow IT organizata mund të mos ekspozohet ndaj rreziqeve ose mund të ekspozohet ndaj një rreziku kritik. Organizata thjesht nuk e ka këtë informacion. Prandaj, Shadow IT konsiderohet një rrezik i pamenaxhuar.

TIPET E SHADOW IT

Ky seksion përshkruan mënyrat kryesore që Shadow IT mund të shfaqet në organizatën tuaj dhe kërcënimet që kjo mund të sjellë

Pajisjet e pamenaxhuara

Shadow IT përfshin pajisje të paautorizuara që kanë akses në rrjet, të cilat mund të përfshijnë:

- pajisjet personale që u përkasin punonjësve në rrjetin kryesor të organizatës
- pajisje që ofrojnë një shërbim kritik dhe nuk janë konfiguruar mirë
- IoT ose pajisje të tjera inteligjente që punonjësit i përdorin pa një miratim sigurie (zilet inteligjente, asistentë digjitalë, printera, etj.)
- servera ose VM-të e sjella nga punonjës (ose kontraktorë) për të ofruar një shërbim pa miratim

Çdo pajisje ose shërbim që nuk është konfiguruar nga organizata juaj ka të probabilitet të mos përmbushë standardet e kërkuara të sigurisë dhe mund të dëmtojë rrjetin dhe shërbimet tuaja. Ato gjithashtu mund të futen në rrjete botneti ose të përdoren si *cryptominers*, duke shkaktuar dëme shtesë.

Shërbimet e pamenaxhuara

Shadow IT në Cloud mund të përfshijë:

- shërbime të pamiratuara të shkëmbimit të mesazheve ose videokonferencave
- shërbimet e jashtme të shërbimit CLOUD për të ndarë dokumentat me palët e treta (ose për të lejuar stafin të punojë nga shtëpia duke përdorur një pajisje të paautorizuar)
- përdorimi i aplikacioneve të palëve të treta që mund të mbledhin informacione të organizatës
- mjediset e pamenaxhuara të cloud të përdorura nga zhvilluesit si mjedise testimi
- shërbime për menaxhim projektesh ose planifikim objektivash që përdoren në vend të mjeteve që ka në dipozicion organizata

Kërcënimet që paraqet Shadow IT

1. Vjedhja e të dhënave

Shumë nga kontrollet që organizatat aplikojnë për pajisjet dhe shërbimet (si enkriptimi dhe allow/deny listing) nuk zbatohen në mënyrë efektive në Shadow IT.

Mbrojtja e të dhënave është e rëndësishme, pasi nuk mund të jeni të sigurt se ku janë të dhënat tuaja, ku po përpunohen ose ku përfundojnë. Nëse nuk keni kontrollin e shërbimeve që përpunojnë të dhënat (ose pajisjet që mbajnë të dhëna), nuk mund të jeni të sigurt që po bëhen kopje rezervë në mënyrë të përshtatshme. Kjo mund ta ekspozojë një organizatë ndaj kërcënimit të ransomware, çështjeve ligjore rreth trajtimit të të dhënave, dëmtimit të reputacionit dhe kostove të rikuperimit.

2. Shfrytëzimi i shërbimeve ose pajisjeve

Kontrolle të tilla si firewall-e të konfiguruara mirë, lista e aplikacioneve të lejuara, softueri antivirus dhe autentifikimi me shumë faktorë (MFA) mund të ndihmojnë në uljen e rrezikut të kompromentimit.
Për Shadow IT, nuk mund të supozohet se këto kontrolle janë zbatuar. Kjo nuk vlen vetëm për pajisjet tradicionale të punës (të tilla si telefonat, laptopët dhe PC-të), por edhe pajisjet e integruara që kanë një lidhje interneti. Kjo mund të ekspozojë një organizatë ndaj kërcënimeve nga malware (duke përfshirë ransomware) dhe monitorimit të paautorizuar të rrjetit.

KUNDËRMASAT PËR SHADOW IT

Në çdo kohë, duhet të përpiqeni në mënyrë aktive të kufizoni mundësitë që Shadow IT mund të krijohet në të ardhmen, jo vetëm të adresohen rastet ekzistuese.

Kundërmasa organizative

Është e rëndësishme të ritheksohet se shumica e rasteve të Shadow IT nuk vijnë si rezultat i shkeljes së qëllimshme të rregullave, por si rezultat i përpjekjeve të stafit për të 'kryer punën e tyre' aty ku pajisjet dhe shërbimet e ofruara nga organizata nuk janë të mjaftueshme. Në shumë raste, stafi mund të mos e kuptojë se po e vë organizatën në rrezik.

Organizatat duhet:

- të shmangin bllokimet e panevojshme të aplikacioneve. Nëse mund të parashikoni nevojat e përdoruesve tuaj, mund të jeni në gjendje të parandaloni fillimin e Shadow IT.
- të zbatojnë një procesi efektiv dhe të thjeshtë për adresimin e kërkesave të përdoruesve, i cili duhet të zbatohet sa më shpejt që të jetë e mundur. Përsëri, nëse përdoruesit nuk mendojnë se nevojat e tyre po adresohen menjëherë, kjo i inkurajon ata të zbatojnë zgjidhjet e tyre.
- të kenë procese ku përdoruesit mund të kenë shpejt akses në shërbimet që mund të jenë jashtë asaj që është normalisht e disponueshme, në një mënyrë të kontrolluar, dhe që mund të vihen nën kontroll gjithnjë e më të lartë sipas nevojës.
- të zhvillojnë një kulturë efektive të sigurisë kibernetike, në mënyrë që stafi të jetë në gjendje të komunikojë hapur rreth çështjeve, duke përfshirë këtu rastet kur politikat aktuale ose proceset po i pengojnë ata të punojnë në mënyrë efektive. Një kulturë e shëndetshme e sigurisë kibernetike shton mundësitë që njerëzit të raportojnë raste të Shadow IT. Ata do të hezitojnë të raportojnë nëse do të kenë frikë se ata (ose anëtarët e tjerë të stafit) do të qortohen. Me fjalë të tjera, një kulturë e dobët e sigurisë do të thotë që ju keni shumë më pak gjasa të zbuloni Shadow IT.

Kundërmasa teknike

Ekzistojnë një sërë teknologjish dhe zgjidhjesh komerciale që mund t'i ndihmojnë organizatat të menaxhojnë rrezikun e Shadow IT në rrjetin e tyre.
Kjo përfshin certifikatat X.509, menaxhimin e aseteve, skanerët e rrjetit etj

Kontrollet e aksesit në rrjet

Një nga kontrollet më pak efektive për të parandaluar punonjësit të lidhin pajisje të paautorizuara janë kontrollet e larta të aksesit në rrjet.
Kontrollet më efektive përdorin certifikata kriptografike të lëshuara për pajisjet. Certifikata X.509 është një certifikatë digjitale që përdor standardin ndërkombëtar të pranuar gjerësisht të infrastrukturës së çelësit publik X.509 (PKI) për të verifikuar që një çelës publik i përket identitetit të përdoruesit, kompjuterit ose shërbimit që përmban certifikata.

Menaxhimi i aseteve

Sistemet e menaxhimit të aseteve përfshijnë informacione kyçe , të cilat përfshijnë detajet fizike të pajisjes, detajet e vendndodhjes, detajet e versionit të softuerit, pronësinë dhe informacionin e konektivitetit (siç janë emri i hostit, adresa IP, MAC adresat e adaptorit të rrjetit, etj.).

Skanerat e rrjetit

Organizatat duhet të jenë të vetëdijshme se ka rreziqe për t'i dhënë privilegje një skaneri rrjeti dhe aftësinë për të skanuar të gjitha elementët e rrjetit, duke e bërë vetë skanerin një objektiv të vlefshëm për sulmuesit.