# Kuidas kindlustada vundamenti ehk Active Directory turvalisusest viimaste küberrünnakute taustal

7 aastat tagasi - 05.04.2019 Autor: Mart Kiilas

Liiga vähe on tähelepanu pööratud Active Directory turvalisusele, kuigi suure osa Eesti ettevõtete jaoks on AD näol tegu IT vundamendiga, millele kõik muu toetub.

## Rünnakud, mis on juba toimunud

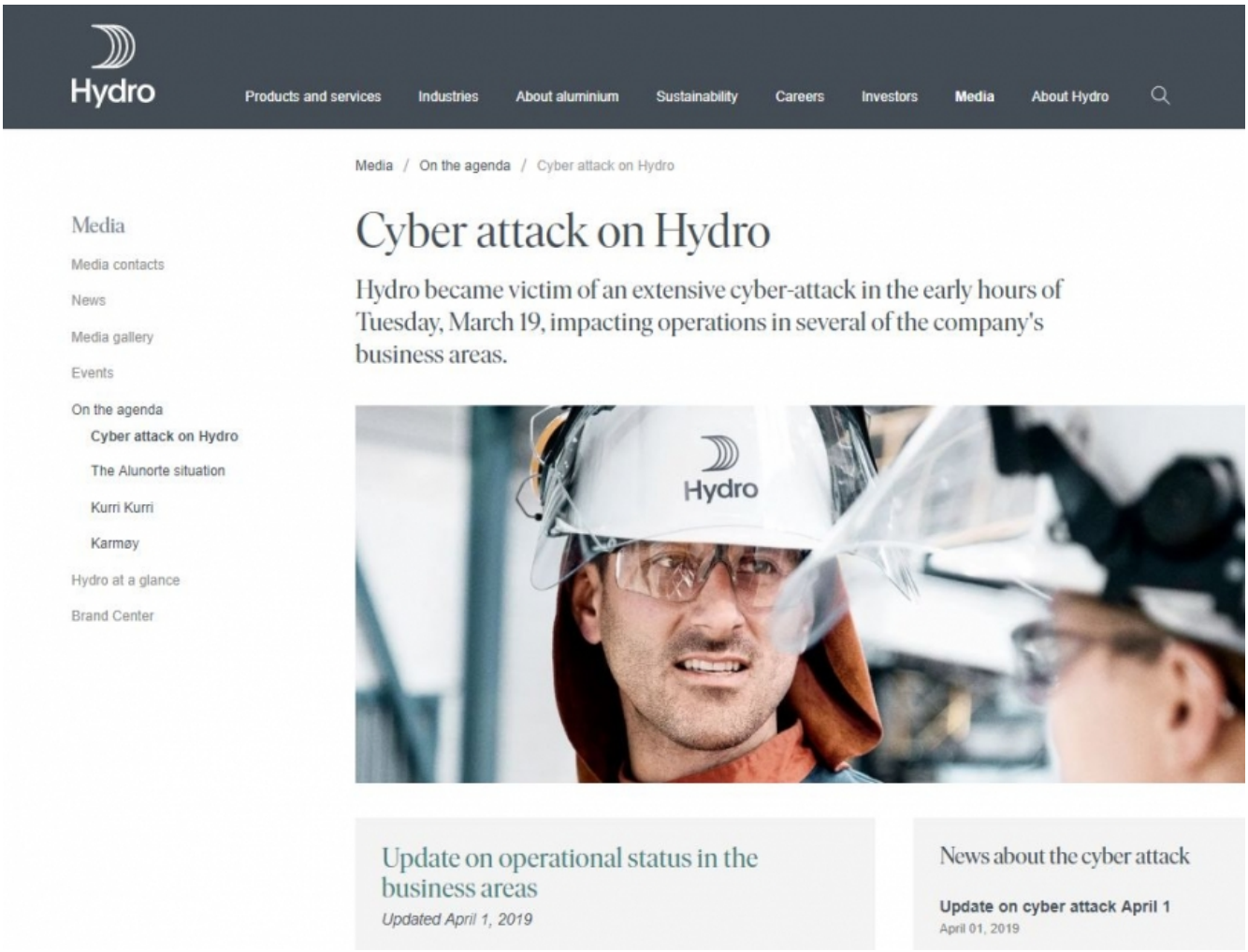
19. märtsil sattus küberrünnaku alla üks maailma suurimaid alumiiniumitootjaid, 35 000 töötajaga börsiettevõte Norsk Hydro. Lunavara krüpteeris suure osa arvutitest, nii et ettevõtte IT-süsteemid lakkasid toimimast. Automaatjuhtimisel olev tootmine jäi seisma ning seda üritati üle viia käsitsijuhtimisele. Tänase päevani ehk rohkem kui kaks nädalat hiljem ei ole veel kõiki süsteeme tööle saadud. Samuti pole kogu tootmisvõimsust taastatud. Ettevõte ise on teada andnud, et kahjusumma jääb suurusjärku 35 miljonit eurot.

Positiivsena tuleb mainida, et firma otsustas esimesest päevast peale informeerida avalikkust ning iga päev anti olukorra muutuste kohta tagasisidet.

Jaanuaris sai sama viirusega pihta Prantsuse inseneriettevõtte, 34 000 töötajaga Altran Technologies, kus viirus halvas samuti kõik IT-süsteemid.

Kaks Ameerika keemiaettevõtet, Hexion ja Momentive, nakatusid LockerGoga viirusega 12. märtsil ja Momentive'i puhul oli tagajärjeks „global IT outage".

## Mis Norsk Hydros juhtus?




Norra CERTi väitel saadi ühel või teisel moel ligi D*omain Administrator* kontole ja on spekuleeritud, et viirus saadeti laiali AD grupipoliitikaga. Ei ole veel selgunud, kuidas pääseti ettevõtte võrku. Viirusetõrjest mingit kasu ei olnud, sest sel hetkel veel ükski viirusetõrje konkreetset LockerGoga versiooni tuvastada ei suutnud.

## Kahjud on hiiglasuured

Järjest enam näeme, et küberintsidendid toovad kaasa kogu arvutipargist ilmajäämise. Järjest enam näeme ka seda, et ettevõtte töö taastamine võtab aega mitte tunde ega päevi, vaid nädalaid ja kuid.

Et kahjud maanduvad otse kasumireal, siis on ettevõtete juhtide ja omanike asi tagada IT-osakonnale vajalik ressurss probleemide ärahoidmiseks.

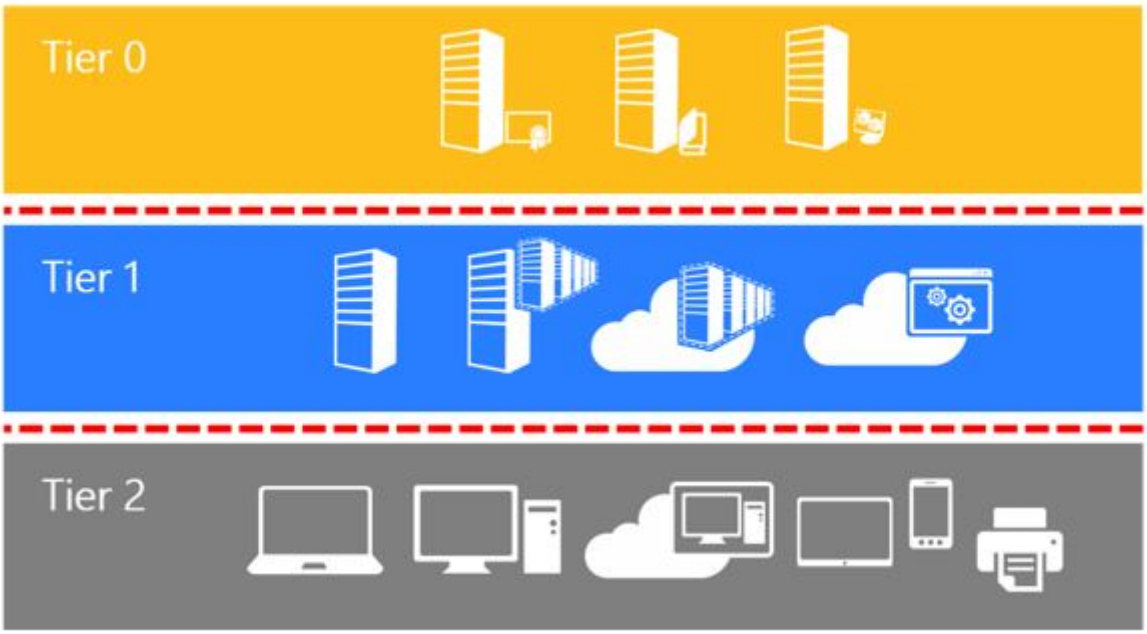
Kahjud lähevad aga järjest suuremaks – näiteks logistikaettevõtte Maersk 300 miljonit dollarit, ravimitootja Merck 285 miljonit dollarit (PDF). Eestiga seoses kandis ehitusettevõte Saint Gobain/Ehituse ABC kahju 220 miljonit dollarit.

## Kuidas sinu ettevõte saab vältida samasugust olukorda?

Enamik lunavararünnakuid ja eelmainitud küberintsidente juhtus sellepärast, et ignoreeriti Microsofti parimaid praktikaid ja elementaarset IT-hügieeni, mitte sellepärast, et neid ettevõtteid oleks tabanud erakordne ebaõnn.

Ühine joon kipub olema see, et IT-osakond on omaenda kontodega lohakalt ümber käinud.

Tavaliselt saab küberintsidendi riski märkimisväärselt vähendada juba olemasolevate vahenditega, kui neid õigesti seadistada. Suurte summade tampimine infrastruktuuri ei ole tingimata vajalik. Active Directory (AD) on sul olemas ja sellega tuleb kaasa lugematu arv turvatehnoloogiad, mida saad tasuta kasutusele võtta.




Alusta Active Directory Tier mudeli juurutamisest:

- Loo eraldi kontod domeenikontrolleris, serverites ja tööjaamades kasutamiseks.
- Kasuta eraldi ilma eriõigusteta kontot internetis surfamiseks ja e-maili lugemiseks.
- Tee OU-de struktuur Tier-mudelile vastavaks.

Windowsi näol on sul olemas operatsioonisüsteem, millel samuti arvukalt võimalusi turvalisuse suurendamiseks. Alusta sellest, et kõik IT-spetsialistid teevad igapäevast tööd ainult PAW (https://aka.ms/cyberpaw) turvastandardile vastava tööjaamaga ning kasutavad privilegeeritud kontosid ka ainult PAW standardiga masinates.

## Mis on elementaarne IT-hügieen?

Active Directory on iga Windowsi baasil tegutseva ettevõtte kõige olulisem andmebaas ja Domain Admins privileegidega kontodel on seal piiramatuid õigusi. Seetõttu tuleb miinimumini viia nende isikute ja kontode hulk, kellel või millel on piiramatult õigusi. Seejärel tuleb viia miinimumini vektorite hulk, mis võivad kaasa tuua konto kaaperdamise.

Võimalikult suur hulk tegevusi tuleb teha kontodega, millel on madalama taseme õigused. See saavutatakse õigusi delegeerides. Kõik kontod tänapäeva AD-s peavad vastama põhimõttele – ainult vajalikud/minimaalsed õigused töö tegemiseks ja mitte grammigi rohkem.

## Võta õppust!

Tüüpiliste AD nõrkuste kõrvaldamiseks soovitan sul käituda järgmisel viisil:

- Domain Admins kontode hulk vii miinimumini. Helpdesk, IT tugiisikud ja enamik teisi spetsialiste ei vaja töö tegemiseks Domain Admins õigusi. Võlusõna on õiguste delegeerimine. Microsofti parim praktika on kaks DA kontot. Kui mitu on sinu ettevõttes?
- Domain Admins kontosid ei tohi kasutada kuskil mujal kui ainult domeenikontrolleris. Mujal kasutamine peab olema grupipoliitika abil piiratud.
- Domain Admins kontodega ei tohi kolada internetis. See peab olema tehniliste meetmetega (proksi/tulemüüri reeglitega) piiratud.
- Domain Admins kontoga ei loeta e-maile.
- Domain Admins kontod peavad olema parooli aegumisega. Välja arvatud üks konto, mida kasutatakse kriisiolukorras ja mille parool asub seifis.
- Domain Admins kontod tuleb viia kahetasemelise autentimise peale. Välja arvatud üks konto.
- Domain Admins kontode – anonüümsete Administrator, helpdesk, aiku, pets jms – kasutamine tuleb lõpetada. Igal ajahetkel peab olema võimalik tuvastada, kes mingi konto alt tegutseb. Kriisiolukorras võib tekkida vajadus kaasata väliseid eksperte ja siis peab olema spetsialistidel kerge tuvastada, millised kontod on pigem legaalsed ja millised mitte. DA konto parooli ei jagata kellegi teisega.
- Helpdeskil ja IT-tugiisikutel ei tohi olla ligipääsu domeeni administraatori arvutisse ega ühtegi teise Tier 0 seadmesse, samuti ei tohi neil olla õigust hallata Tier 0 taseme ressursse. See on klassikaline sillapea, kust privileege

eskaleeritakse.

- Ära lisa teenuskontosid igaks juhuks privilegeeritud gruppidesse. Ära anna Domain Admins õigusi. Lokaalseks administraatoriks ära tee. Uuri, mis õigusi teenus tegelikult vajab ja lisa ainult need õigused. Pane kindlasti peale „Log On To…“ piirang.
- Vii anonüümsete AD kontode hulk miinimumini ja pane kontodele „Log On To…“ piirang.
- Kõik IT-kontod peavad olema parooli aegumisega. Never Expires kasti linnukest ära pane, see jäägu üheksakümnendatesse.
- Kõik kaugligipääsuga (näiteks VPN, RDP) kasutajad peavad olema kahetasemelise autentimisega. Kasutajate paroole õngitsetakse iga päev ja pole raske ette kujutada, et kellelgi juba on ligipääs teie võrku. Või müüakse seda ligipääsu mustal turul.
- Keegi ärgu kolagu internetis ühegi privilegeeritud kontoga, millega hallatakse servereid või tööjaamu. See peab olema tehniliselt võimatu (proksi/tulemüüri reeglite abil).
- Ei tohi eksisteerida ühtegi universaalkontot, millega pääseb kõigisse tööjaamadesse või serveritesse. Sellised kontod teevad halval päeval sinu keskkonnas lageraie. Märksõna on LAPS paroolilahendus (http://aka.ms/LAPS ).
- Võrgud peavad olema segmenteeritud, et intsident jääks ühe segmendi piiresse ega ohustaks kõiki IT-süsteeme. Kõik pädeva IT-ga organisatsioonid eeldavad, et viirused/häkkerid võivad nende võrku sattuda (tänapäeval lähtutakse Zero Trust mudelist). Kuid vahe on selles, et hea IT-hügieeniga ettevõttes tagab erinevate turvakihtide hulk, et pahalasel ei õnnestu ühest kihist teise edasi liikuda. Ei ühest võrgust teise ega tavakasutajast domeeni administraatoriks. Ning monitooringu kiht (Microsoft ATA, SIEM) tagab, et kahtlased tegevused avastatakse.

Hea IT peab kinni tootja soovitatud parimast praktikast ja fookus on probleemide ennetamisel. Hea IT õpib teiste vigadest. Halb IT reageerib ainult siis, kui tulekahju on käes. Kumba rolli esindab sinu IT?

Teeme Eesti AD-infra kõige turvalisemaks maailmas. Iga okas loeb!

**MART KIILAS**

Süsteemiadministraator

- Lahendused

- Turvalisus

Pilt

