dots.

Organizācijas kiberdrošība mūsdienās ar Zero Trust Framework

(... vai tiešām neticam nevienam?)

Jānis Giniborgs

CERT.LV IT drošības seminārs «Esi drošs»

24.03.2022

Saturs

Zero Trust framework (ZTF) pamatideja –

Nekad
netici, vienmēr pārbaudi!

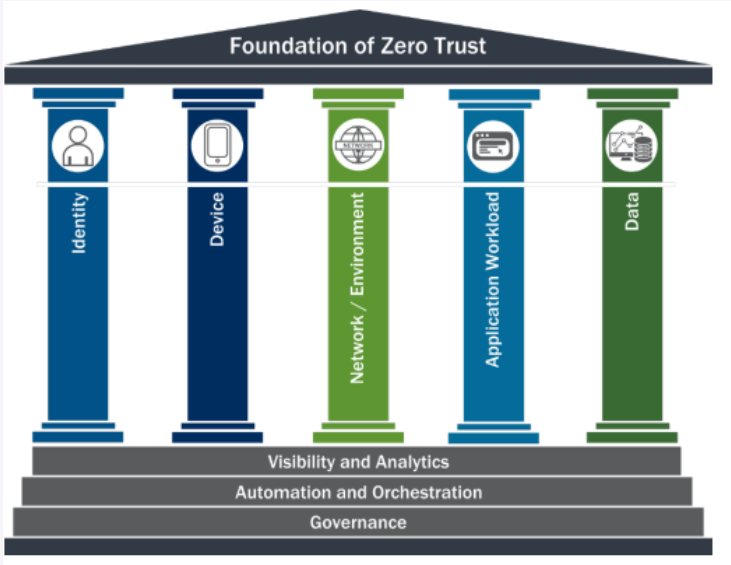
- Pirmās idejas jau 1994.gadā, termins *zero trust* pirmo reizi ieviests 2010.gadā.
- Tiek pieņemts, ka ārējais perimetrs, ja arī vēl eksistē, faktiski nepasargā (ir kompromitēts), un tāpēc aizsardzība ir jāveido jau katram konkrētajam infrastruktūras elementam.
- Apkopo idejas un konceptus, kā pasargāt organizācijas informāciju sistēmas un datus mūsdienu vidē, kad draudi nāk no dažādiem avotiem.
- Balstās uz 5 (6) pīlāriem.

ZTF pīlāri

- IDENTITĀTE - lietotāju, servisu un iekārtu identitātes pārvaldība.
- TĪKLS/INFRASTRUKTŪRA - datortīkla un infrastruktūras iekārtu arhitektūra un pārvaldība.
- DATI - datu pārvaldība.
- PROGRAMMATŪRA - aplikāciju arhitektūra un pārvaldība.
- IEKĀRTAS - gala iekārtu pārvaldība, t.sk. darbs no mājas datoriem un cita veida nepārvaldīto iekārtu scenāriji.

Kas ir ZTF brieduma modelis?

- Lai kaut kur nokļūtu, ir jāsaprot pašreizējā situācija un iespējamais ceļš uz mērķi.
- Brieduma modelis ļauj to novērtēt.
- Vērtē katru pīlāru, bet svarīgs ir konteksts.
- Ir pieļaujama situācija, kad atsevišķi elementi atsevišķos pīlāros nav optimāli.



ZTF brieduma pakāpes

1

Sākotnēja vai tradicionāla – manuālas konfigurācijas un atribūtu piešķiršana, statiska drošības politika, minimāla starpsistēmu sadarbība, manuāla resursu piešķiršana, proprietāri un neelastīgi politiku īstenošanas risinājumi, manuāla un reaktīva reaģēšana uz incidentiem un to seku mazināšana.

2

Uzlabota vai progresīva – notiek koordinācija starp pīlāriem, ir ieviesta centralizēta redzamība, centralizēta identitātes kontrole; drošības kontroļu politikas īstenošana, kas balstīta uz datiem un notikumiem citos griezumos; incidentu pārvaldība, balstoties uz predefinētām darbībām; daži tiesību ierobežojumi tiek balstīti uz precīziem amata novērtējumiem.

3

Optimāla – pilnībā automatizēta atribūtu piešķiršana iekārtām un resursiem, dinamiska drošības politika, kas balstīta uz automatizētiem notikumu trigeriem, resursiem ir dinamiskas privilēģijas piekļuvei (atbilstoši noteiktiem sliekšņiem), tiek pielietoti atklāti standarti starp pīlāru sadarbspējai.

Brieduma vērtēšana

Katrs pīlārs tiek sadalīts 6-7 apakškategorijās, lai vērtējums būtu precīzāks. Piemēram, datortīklam pamata kategorijas ir:

- segmentācija;
- draudu kontrole tīklā;
- pārraidīto datu šifrēšana.

Papildus visiem elementiem kopīgi piemērojamās kategorijas ir – monitorings un analītikas iespējas, operāciju automatizācijas un pārvaldības līmenis.

Kā to pielietot praksē?

- Sākotnējais brieduma novērtējums ļauj ne tikai apzināt situāciju, bet arī redzēt, kas tieši pietrūkst, lai pārietu uz nākamo līmeni.
- Jāizvērtē ir visi pīlāri, lai identificētu nopietnākos trūkumus.
- Brieduma vērtēšana ļauj prioritizēt drošības pasākumus, vērtējot no esošo ieguldījumu viedokļa un organizācijas kopējās IT stratēģijas (kuru varbūt vērts mainīt?).
- Brieduma modeļu kontroles saraksti ir brīvi pieejami internetā – CISA, Microsoft lapās.

Ieguvumi no brieduma vērtējuma

1. Apzināta «lielā bilde», nevis konkrēti trūkumi
2. Identificēti apgabali, kuros nosacītā atpalicība rada lielākos riskus
3. Apkopoti skaidri ieteikumi, kā labot situāciju
4. Ceļa karte organizācijas kiberdrošības stratēģijas izveidei

Piemērs – drošs datortīkls #1

Standarta situācija – cīnāmies ar perimetra aizsardzību, iekšpusē apakštīklu sadalījums ir pamatā formāls, serveru segmenta nodalīšana veikta *VLANu* līmenī ar triviāliem *access lists*, tehniski organizācijas telpās iespējams pievienot jebkādu iekārtu tīklam, tīklā var eksistēt koplietošanas mapes bez autentifikācijas, iekštīkla datu plūsmas netiek kontrolētas.

Piemērs – drošs datortīkls #2

Pašlaik par drošu uzskatītais modelis:

- ieviešam detalizētu ienākošā satura filtrāciju uz ugunsmūra/proxy;
- ieviešam tīkla pieejas kontroles (NAC);
- ieviešam tīkla IDS;
- ieviešam SIEM un vācam lielu daudzumu pierakstu no tīkla iekārtām, mēģinām ar to visu tikt galā (meklējam drošības analītiķus, analizējam pierakstus, apstrādājam incidentus, dzenājam lietotājus);
- vienlaicīgi iekštīklā serverus nodalot no darbstacijām ar atsevišķu ugunsmūri un arī papildus ieviešot mikrosegmentāciju.

Piemērs – drošs datortīkls #3

Optimāls – iekštīkls (lietotāju) ir minimāli nodalīts no ārējā interneta, tas pamatā kalpo kā transports darbstaciju piekļuvei internetam.

- Serveri un aplikācijas ir izvietoti pilnībā nodalītā apakštīklā, kurā vispār nav lietotāju iekārtu un kas tiek izvietots atsevišķā fiziski un loģiski nodalītā datu centrā.
- Aplikāciju pieejas tiek nodrošinātas caur publisko internetu vai VPN!
- Koplietošanas datu glabāšanai tiek izmantotas mākoņservisu mapes, kuras pieejamas tikai autentificētiem lietotājiem.
- Visas lietotāju gala iekārtas tiek centralizēti pārvaldītas, tām ir ieslēgta šifrēšana, regulāri jauninājumi, centralizēta pretvīrusu aizsardzība.

Papildus iespējas mūsu klientiem

1. MK442 atbilstības pašvērtējuma rīks **ej.uz/MK442**

2. Esam izstrādājuši ZTF brieduma vērtējuma lokalizāciju, kur atbilstošu pārbaudi varam veikt klientiem, kuriem nepieciešams kiberdrošības risku mazināšanas un investīciju plāns.

dots.

wearedots.com
+371 67509912
info@wearedots.com