Kritisko sistēmu lietotāju riski

Arvis Berkolds

Drošības risinājumu konsultants

Šodien jums pastāstīšu:

1. Vai kritiskā infrastruktūra ir tas pats, kas kritiskās sistēmas?
2. Kādi ir apdraudējumi?
3. Kritisko sistēmu lietotāju un privilēģiju riski, un kā tos samazināt
4. Izplatītākie lietojuma konti un to pielietojums
5. Realitāte pret ilūzijām
6. Kopsavilkums – ko darīt, ja vajag darīt

Drošība

Centralizācija

Digitalizācija

Kiberdraudi

Pārvaldība

Uzbrukumi

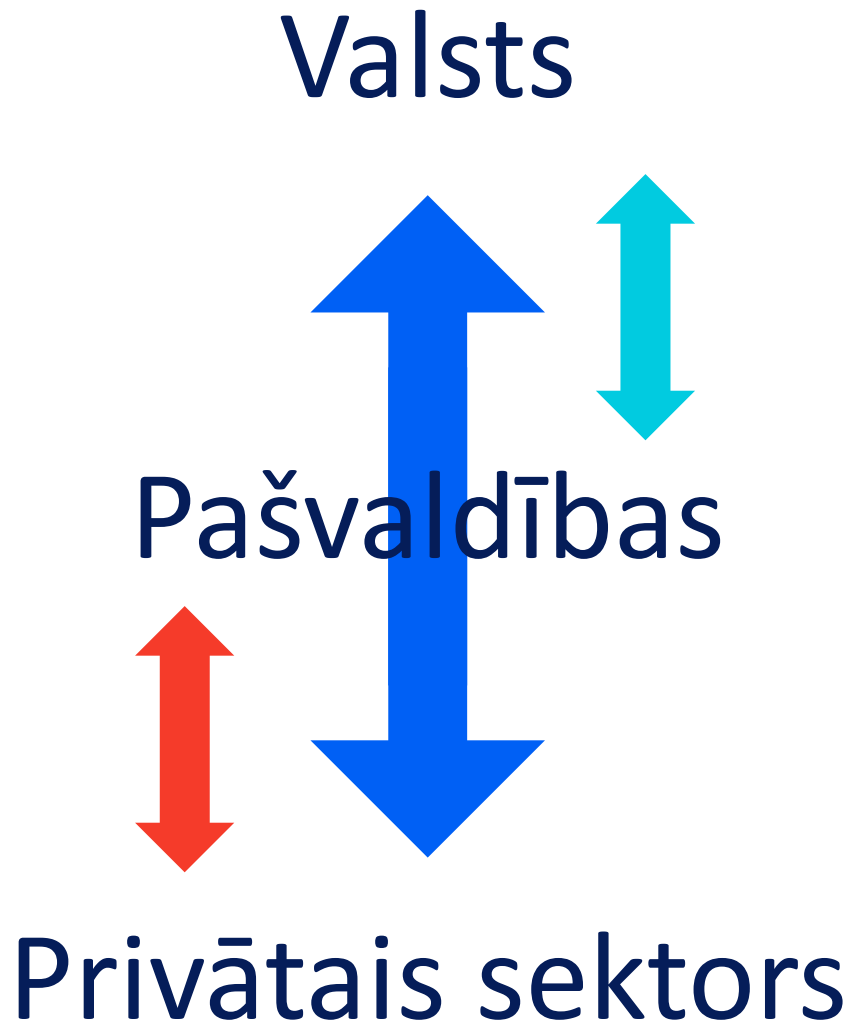
Sistēmas

Draudi

Resursi

Transformācija

Riski



Informācijas aprite

Kritiskā infrastruktūra, kritiskās sistēmas!

Kritiskā infrastruktūra un sistēmas

Valsts informāciju sistēmas

Maksājumu un grāmatvedības sistēmas

Datu glabātuves, rezerves kopijas

Klientu un personas datu sistēmas

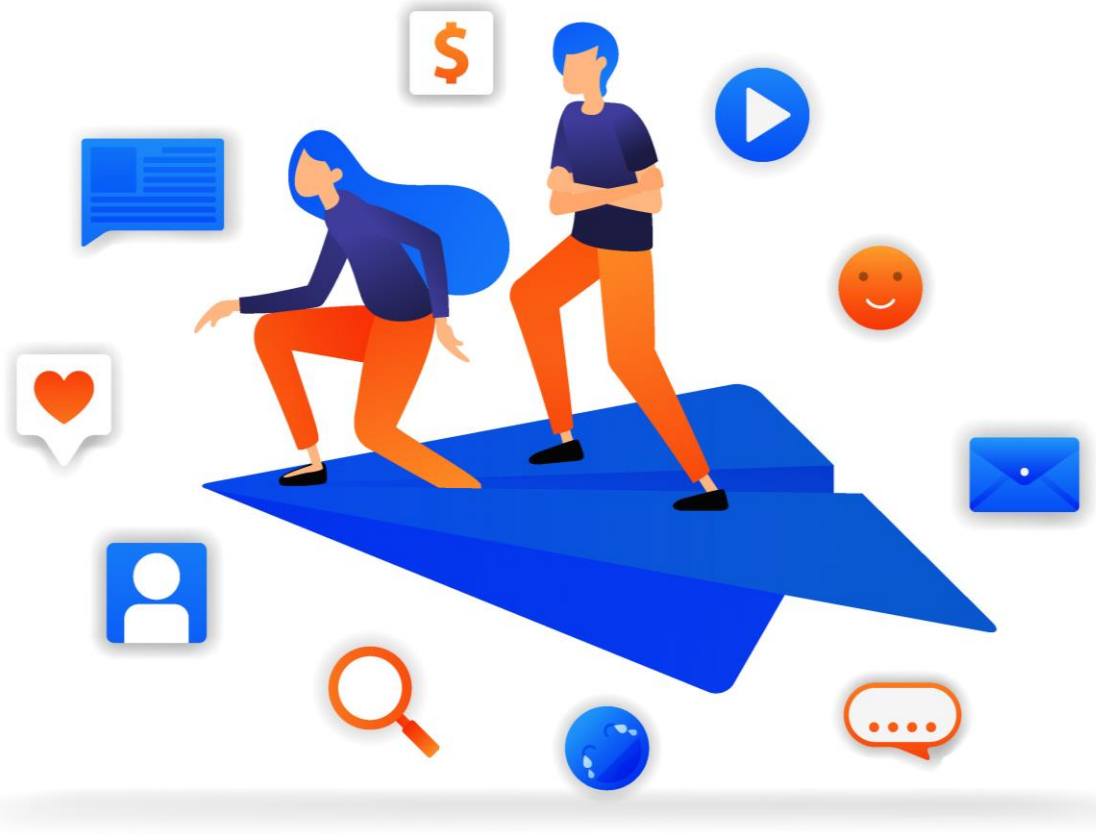
Veselības un aprūpes sistēmas

Tīkla infrastruktūra

Apdraudējumi

- Ļaunprātīga programmatūra
- Pikšķerēšanas uzbrukumi
- Lietu interneta (IoT) ierīces
- Mobilās iekārtas
- Pašu darbinieki
- Galvenā vai administratora konta privilēģijas
- Neizlabotas drošības ievainojamības (patch)
- Ārējie uzbrukumi (ģeopolitiskā situācija)

Kritisko sistēmu lietotāju un privilēģiju riski



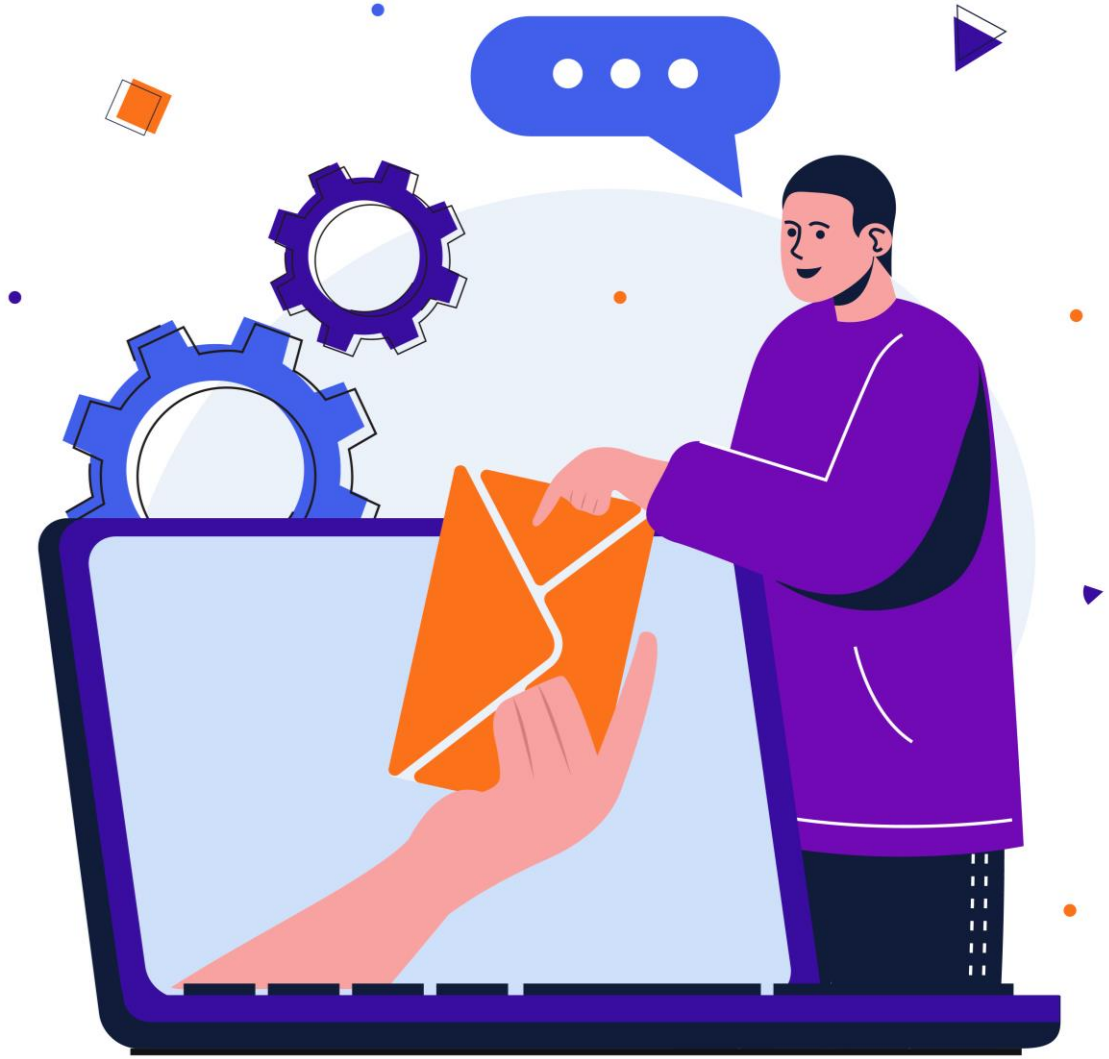
Ierobežota lietotāju redzamība

Pārāk daudz privilēģiju

Autentifikācijas problēmas

Paroļu uzlaušanas ātrums pēc paroles veida, garuma un dažādības

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years



Trešās puses drošības izaicinājumi

Pieslēgšanās ātrums

Kritisko sistēmu lietotāju un privilēģiju riski

Izplatītākie lietojuma konti un to pielietojums!

Izplatītākie lietojuma konti un to nozīmīgums.

Vietējo administratoru konti	Priviliģēto lietotāju konti	Domēnu administratoru konti
Ārkārtas konti	Pakalpojumu konti	Lietotājprogrammu konti

Kāpēc priviliģēto lietotāju pārvaldības risinājums ir svarīgs?


Realitāte pret ilūzijām!

1. Administratoram ir tikai priviliģēts konts.

2. Administratoram ir gan standarta, gan priviliģēts konts.


smith_01!
creditCard
Facebook
Log:Sarah420!
STEALING
PERSONAL
DATA
***
Student loan
WiFi Router

Realitāte pret ilūzijām

80% datu pārkāpumu ir saistīti ar apdraudētiem priviliģēto kontu akreditācijas datiem, piemēram, parolēm, atslēgām un sertifikātiem*;

63% IT profesionāļu apgalvo, ka priviliģēti lietotāji rada maksimālo iekšējās drošības risku**.

*The Forrester Wave: Privileged Identity Management, Q3 2019.

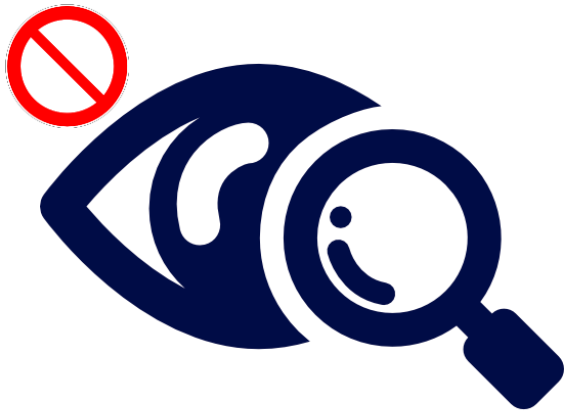
**Cybersecurity Insiders' 2020 Insider Threat Report.

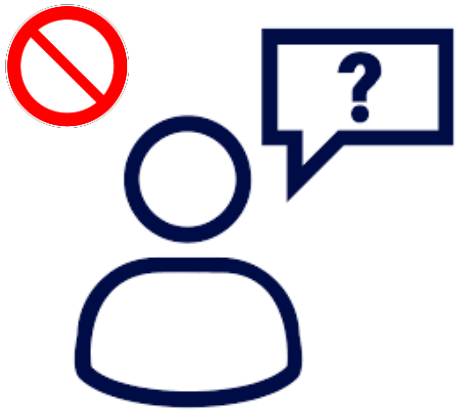

RIGHT
WRONG

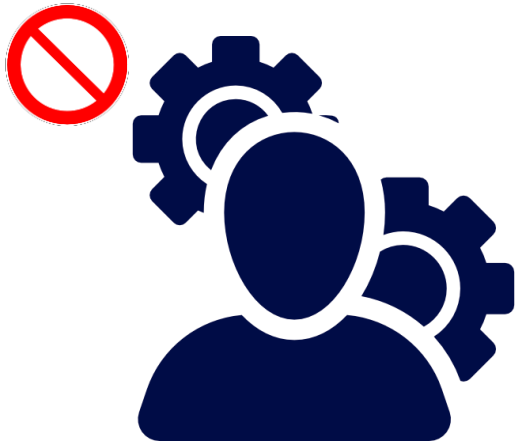
Priviliģētās piekļuves pārvaldības (PAM) risinājums

Ko darīt!

Ko nedarīt!







Paldies!

Arvis Berkolds

Drošības risinājumu konsultants