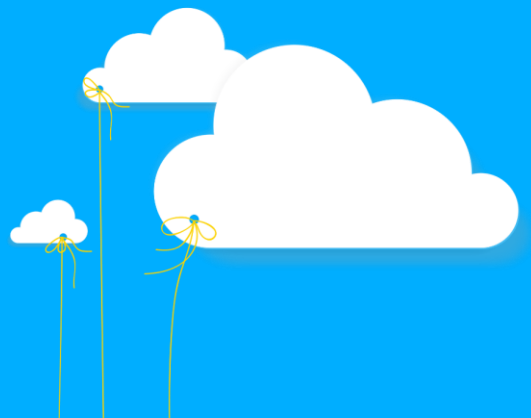
Laukti (ne)galima:

Duomenų saugumo svarba bei galimi sprendimai

Audrius Žemgulis, Technikos direktorius



AUDRIUS ŽEMGULIS

>15 metų CTO

>10 metų CISSP (Certified Information Systems Security Professional)

>2 years CDCMP (Certified Data Center Management Professional)

ISO/IEC 27001, ISO/IEC 20000, PCI-DSS, ITIL ir personalo valdymas – **tai mano darbas.**

Networking‘as, Python, Linux **– tai mano hobiai.**

Zoho plugs another critical security hole in Desktop Central

By **Sergiu Gatlan** January 17, 2022 01:04 PM 0

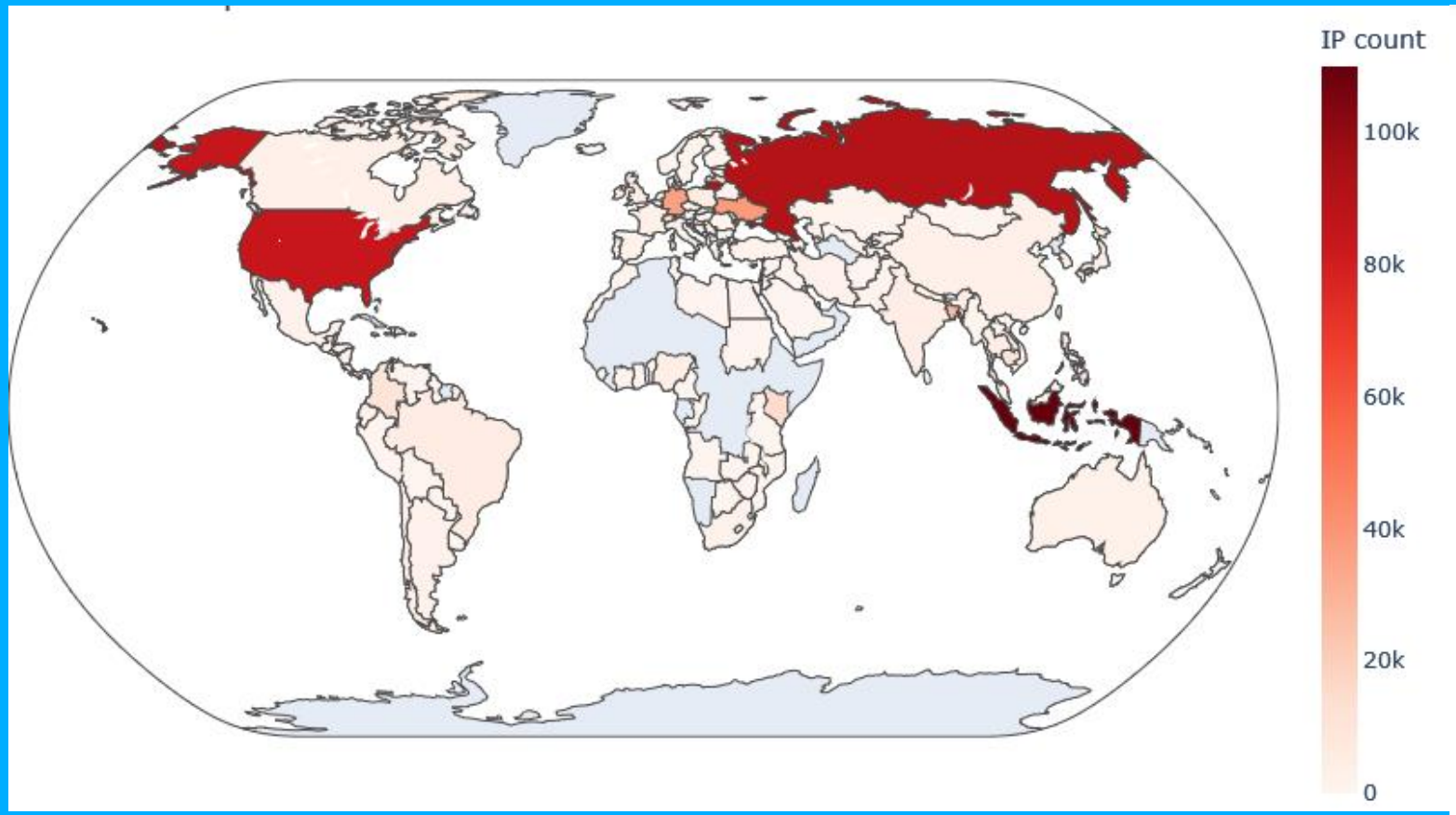
Log4J vulnerability

- Introduced in 2013
- Vulnerability "discovered" in 2021

Zero-Day

Palo Alto Warns of Zero-Day Bug in Firewalls Let Hackers Execute an Arbitrary Code Remotely

By **Balaji N** - November 12, 2021 0



28 Июня 21:17

Россия / Мир / Политика / Новости

Госорганы Литвы подверглись хакерской атаке

Фото: globallookpress.com/Peter Schatz

Автор: Редакция Новоросинформ

Российская хакерская группировка Killnet в своем Telegram-канале сообщила, что за 39 часов хакеры добились блокировки 70% всей сетевой инфраструктуры Литвы, пишет "Лента".

В сообщении от Killnet говорится, что интернет-инфраструктура Литвы находится в блокаде, основная ее часть отключена от мира.

Хакеры сообщили, что блокировке подвергся литовский провайдер Balt Net, а также сайт, приложение и онлайн-сервис самой большой сети АЗС Baltic Petroleum.

Tuo tarpu realybėje...

Saugumo pažeidimai vyksta kiekvieną dieną ir nesvarbu domimės mes tuo ar ne

Resursų turime ribotai

Mažiau rūpi jie mums, kol mūsų tai neliečia

Didžioji dalis aukščiausio lygio vadovų norėtų apsaugoti savo organizaciją vykdant tik tas veiklas, kurios yra būtinos, bet ne perteklinės

Niekas nenori būti kita auka, ypač vadovai, atsakingi už organizacijos veiklą

...

Kibernetinis kvadrantas

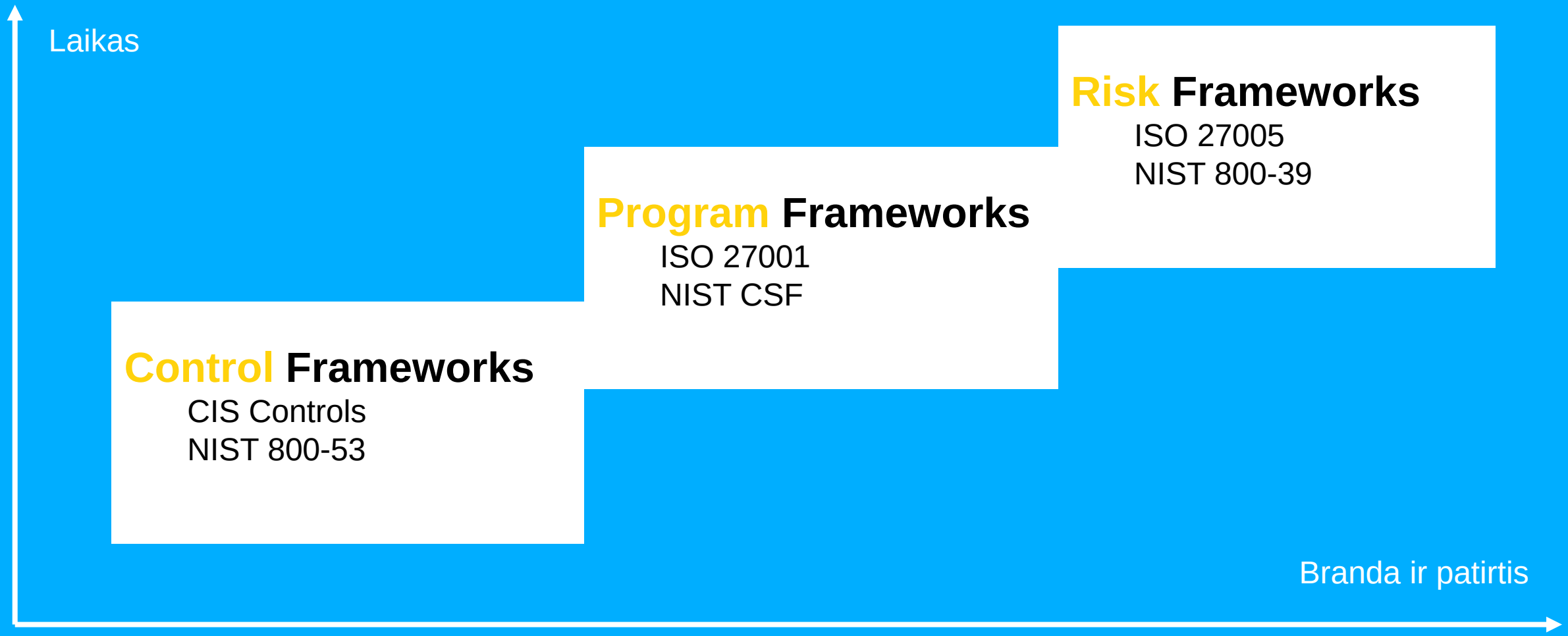
4 levels of cyber resilience

Source: Accenture State of Cybersecurity Resilience 2021, security executives (N=3,455: Cyber Champions N=172, Business Blockers N=522, Cyber Risk Takers N=885, The Vulnerable N=1,876)

	Cyber Champions	Business Blockers	Cyber Risk Takers	The Vulnerable
Gebėjimas sustabdyti atakas: Atakų kiekis su saugumo pažeidimais	1 in 6	1 in 4	1 in 2	1 in 2.3
Pažeidimų identifikavimo greitis: % pažeidimų surastų < 1 dieną	55%	50%	11%	15%
Gebėjimas atstatyti veiklą: % veiklos atstatymų per < 15 d.	100%	96%	30%	30%
Pažeidimų poveikis: % pažeidimų be poveikio veiklai	72%	64%	23%	24%

Source: Accenture State of Cybersecurity Resilience 2021, security executives (N=3,455: Cyber Champions N=172, Business Blockers N=522, Cyber Risk Takers N=885, The Vulnerable N=1,876)

„Vaistas“ saugumo jausmui padidinti – naudoti sistemą



CIS Kontrolės priemonės

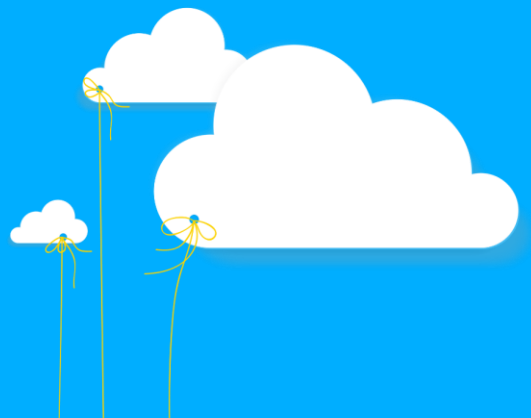
baltneta

Below is a list of the CIS Controls in v8, and how many Safeguards in each are applicable to each Implementation Group.

CONTROL 01 Inventory and Control of Enterprise Assets	5 Safeguards	IG1 2/5	IG2 4/5	IG3 5/5
CONTROL 02 Inventory and Control of Software Assets	7 Safeguards	IG1 3/7	IG2 6/7	IG3 7/7
CONTROL 03 Data Protection	14 Safeguards	IG1 6/14	IG2 12/14	IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software	12 Safeguards	IG1 7/12	IG2 11/12	IG3 12/12
CONTROL 05 Account Management	6 Safeguards	IG1 4/6	IG2 6/6	IG3 6/6
CONTROL 06 Access Control Management	8 Safeguards	IG1 5/8	IG2 7/8	IG3 8/8
CONTROL 07 Continuous Vulnerability Management	7 Safeguards	IG1 4/7	IG2 7/7	IG3 7/7
CONTROL 08 Audit Log Management	12 Safeguards	IG1 3/12	IG2 11/12	IG3 12/12
CONTROL 09 Email and Web Browser Protections	7 Safeguards	IG1 2/7	IG2 6/7	IG3 7/7
CONTROL 10 Malware Defenses	7 Safeguards	IG1 3/7	IG2 7/7	IG3 7/7
CONTROL 11 Data Recovery	5 Safeguards	IG1 4/5	IG2 5/5	IG3 5/5
CONTROL 12 Network Infrastructure Management	8 Safeguards	IG1 1/8	IG2 7/8	IG3 8/8
CONTROL 13 Network Monitoring and Defense	11 Safeguards	IG1 0/11	IG2 6/11	IG3 11/11
CONTROL 14 Security Awareness and Skills Training	9 Safeguards	IG1 8/9	IG2 9/9	IG3 9/9
CONTROL 15 Service Provider Management	7 Safeguards	IG1 1/7	IG2 4/7	IG3 7/7
CONTROL 16 Applications Software Security	14 Safeguards	IG1 0/14	IG2 11/14	IG3 14/14
CONTROL 17 Incident Response Management	9 Safeguards	IG1 3/9	IG2 8/9	IG3 9/9
CONTROL 18 Penetration Testing	5 Safeguards	IG1 0/5	IG2 3/5	IG3 5/5

Prevencija ir duomenų atstatymas

KADA, KAIP, KAS?

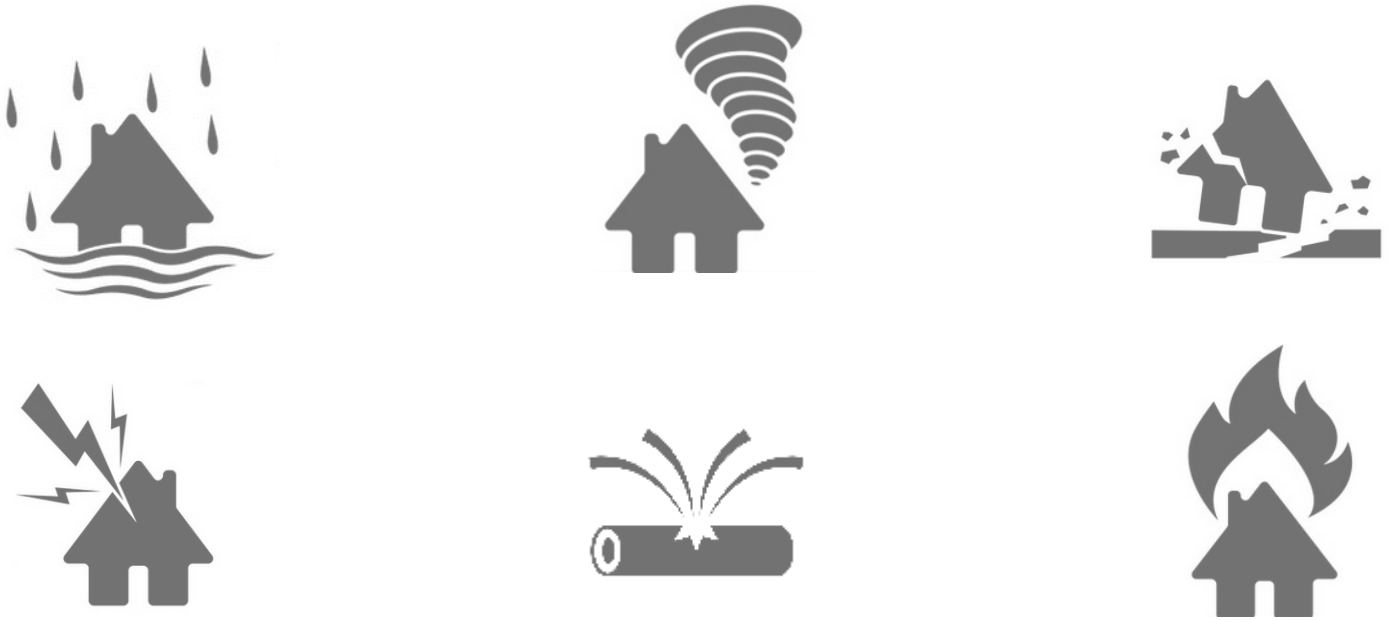


Avarijos

Stichinės nelaimės

5%

Vietinės avarijos



HW, SW, HR, kibernetinės atakos

95%

Ukrainoje...

The New York Times

Hackers Bring Down Government Sites in Ukraine

"Be afraid," warned a message on the defaced Foreign Ministry website, a day after talks between the West and Moscow aimed at preventing a Russian invasion hit an impasse.

The message was posted in three languages — Ukrainian, Russian and Polish — in what seemed like an effort to obfuscate the origins of the hackers and their motives, and shift blame and suspicion elsewhere.

"Ukrainians! All your personal data was uploaded to the internet," the message read. "All data on the computer is being destroyed. All information about you became public. Be afraid and expect the worst." It also raised a number of historical grievances between Poland and Ukraine.

REUTERS

Technology

2 minute read · March 15, 2023 9:09 PM GMT+2 · Last Updated 6 days ago

Russian hackers preparing new cyber assault against Ukraine - Microsoft report

"Since January 2023, Microsoft has observed Russian cyber threat activity adjusting to boost destructive and intelligence gathering capacity on Ukraine and its partners' civilian and military assets," the report reads. One group "appears to be preparing for a renewed destructive campaign."

KADA?

Avarijos metu galvoti apie... NĖRA KADA!

Atstatymo kaštus

Duomenų saugumą

Licencijų perkėlimą

Tinklo pralaidą

Neautorizuotus prisijungimus

Kas už ką atsakingas

Kaip bus pasiekiamos aplikacijos

Kiek laiko tai truks

KADA?

Incidento atveju vienintelis dalykas apie kurį galvojama...

KAIP KUO GREIČIAU PRATĘSTI ĮPRASTUS ORGANIZACIJOS PROCESUS?

Todėl planuoti ir ruoštis reikėjo

VAKAR...

KAIP?

Įtraukite tinkamus žmones

Vadovybė
įvertina poveikį organizacijos veiklai
Darbuotojai
darbuotojų švietimas ir mokymai
Specialistai
vidiniai arba išoriniai

Suklasifikuokite sistemas

Kritinės sistemos
Svarbios sistemos
Testinės aplinkos
...

Pasirinkite tinkamas priemones

Duomenų **saugumui**
Duomenų **saugojimui**
Duomenų **atstatymui**
Veiklos **tęstinumui**

KAIP?

Galima padaryti jau šiandien...

Pagrindinė infrastruktūra

Patikimas duomenų centras

Tinklas | Serveriai | Saugyklos

Atsarginės kopijos

Nutolusios kopijos

„Slaptos“ kopijos

Avarinio atkūrimo sprendimas

Lietuva

Nutolusios kopijos

„Slaptos“ kopijos

Avarinio atkūrimo sprendimas

Europos sąjunga

Nr. 1 debesų kompiuterijos paslaugų tiekėjas Lietuvoje

24/7 dirbantis Klientų aptarnavimo centras bei ISO 20 000, ISO 27 001 procesai

Du duomenų centrai Lietuvoje sertifikuoti Tier3 Design, Facility, PCI DSS

Duomenų centras Frankfurte

Valdoma 1000+ km nuosavo optinio tinklo Lietuvoje. PanBaltic tinklas

160+ darbuotojų
80+ inžinierių

Profesinės civilinės atsakomybės draudimas

Daugiau nei 5400 verslo klientų

Nuo 2015 m. priklausome ATEA įmonių grupei

Ačiū!

www.balt.net