Nevyhnutelná automatizace a řízení certifikátů a důvěryhodných služeb

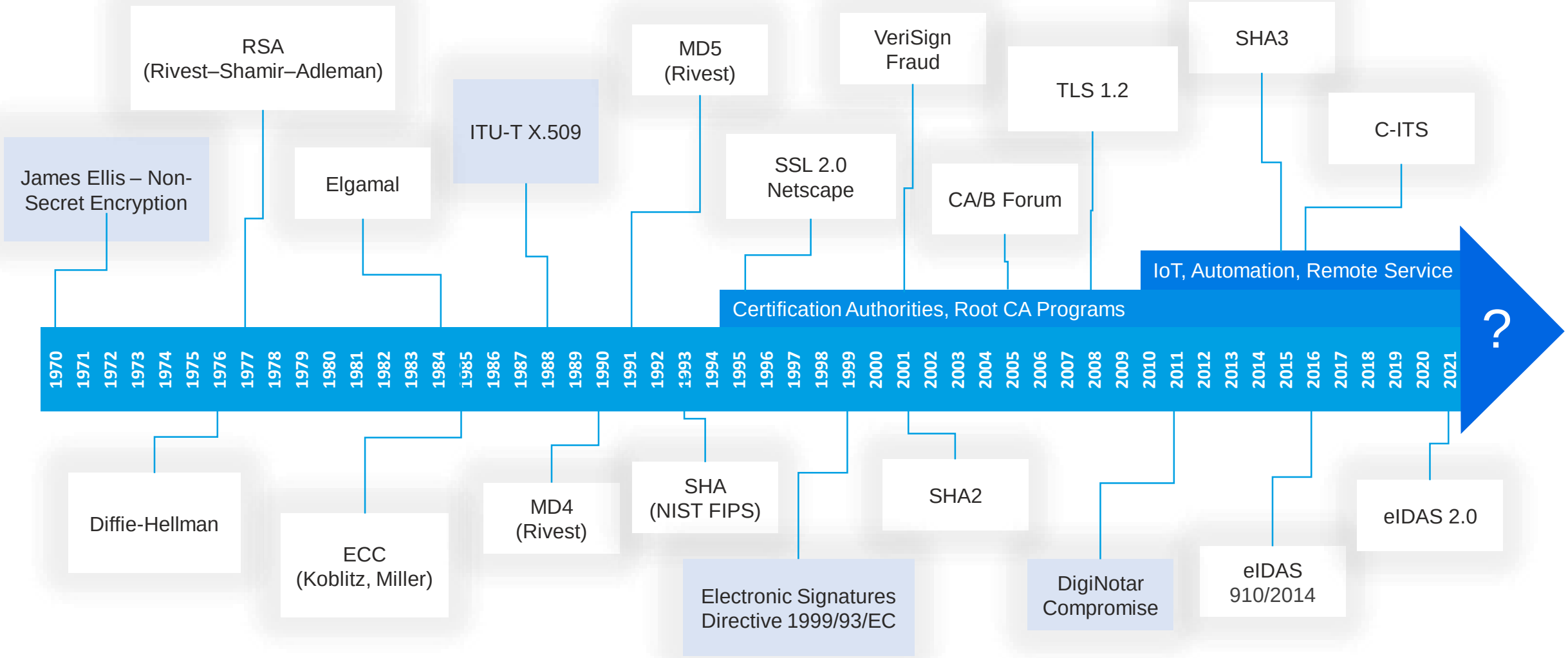
PKI se stává nedílnou a kritickou součástí systémů

14.9.2022

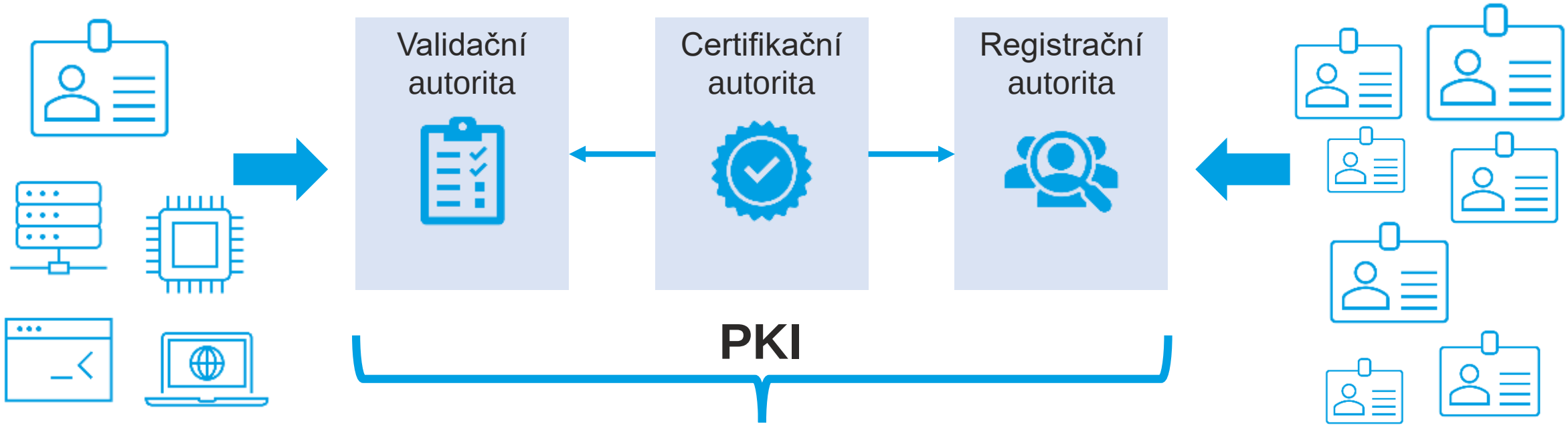
Cybercon Brno 2022

Dalibor Premus

TROCHU HISTORIE



INFRASTRUKTURA VEŘEJNÉHO KLÍČE



Regulátor
Auditor
Root Program

ROSTOUCÍ POČET KLÍČŮ

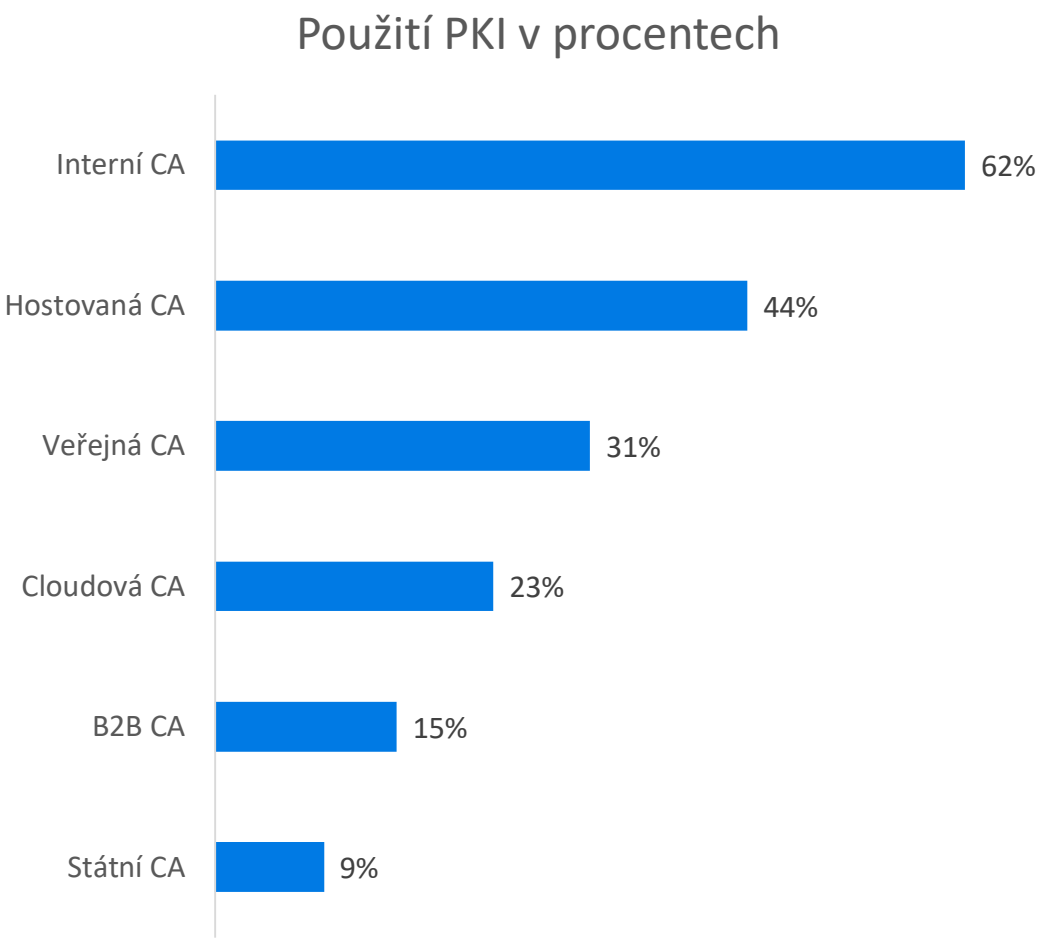
- Infrastruktura veřejného klíče je srdcem bezpečnostního řešení, kde je potřebujete vytvořit nebo zajistit digitální důvěru mezi různými entitami.
- Skládá se nejen z technologie, ale důležitou součástí celku jsou i lidé a postupy.
- IT infrastruktura i aplikace využívají stále více certifikátů k zajištění důvěry a bezpečnosti. Certifikáty jsou stále rozmanitější.

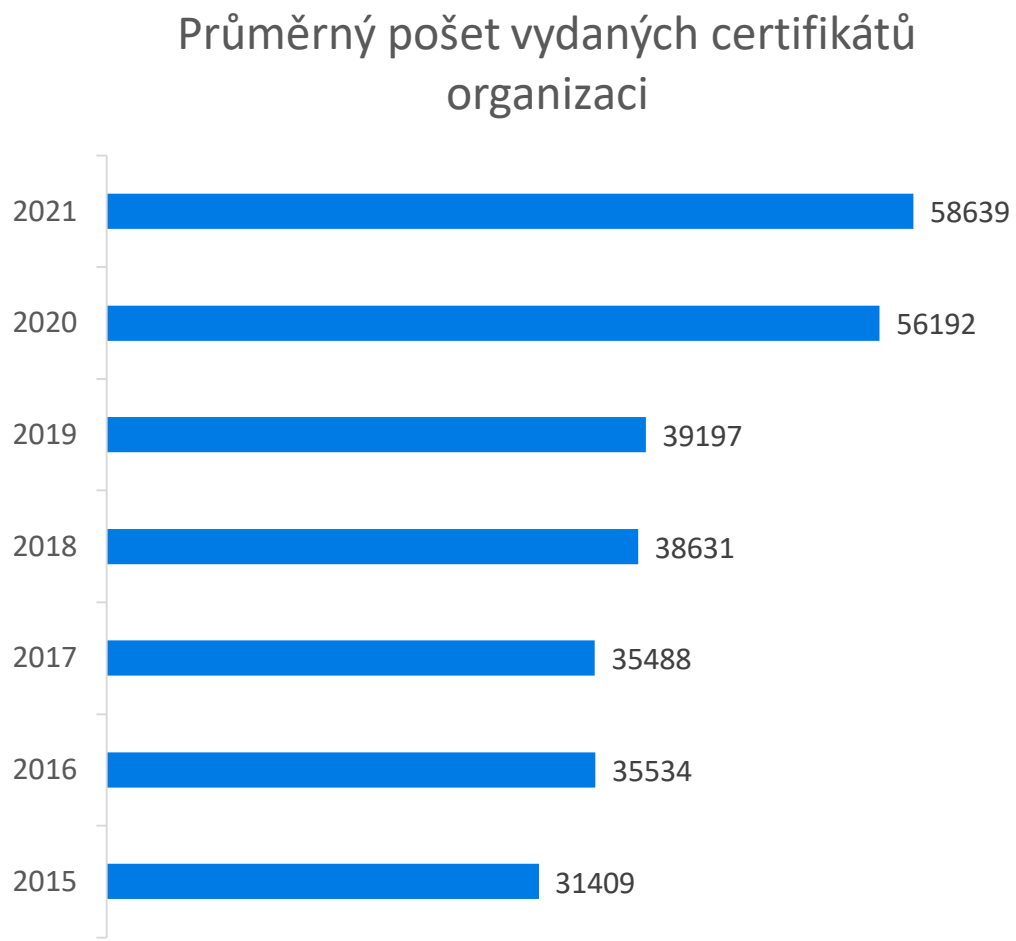
PROČ TOMU TAK JE?

- Přísné standardy a regulace týkající se kybernetické bezpečnosti a ochrany osobních údajů
- Rostoucí obavy ohledně zabezpečení podnikových aktiv duševního vlastnictví (IP)
- Trendy v oblasti Bring Your Own Devices (BYOD)
- Rostoucí počet kybernetických útoků
- Adopce cloudových platforem napříč malými a středními podniky
- Zvyšující se počet IoT zařízení napříč různými průmyslovými vertikálami

Společnosti musí řídit tisíce I miliony digitálních aktiv pro zajištění elektronické identity osob, zařízení a aplikací.

CERTIFIKAČNÍ AUTORITA





* 2021 Global PKI and IoT Trends Study

DŮVĚRYHODNÁ SLUŽBA

- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
  - Elektronická identita
  - Elektronické podpisy, pečetě, razítka
  - Digitální certifikáty
- Důvěryhodná služba je založená na principech kryptografie

Řízení důvěryhodných služeb
(Trust Lifecycle Management)

Řízení kryptografických klíčů (včetně symetrických klíčů!)

Řízení digitálních certifikátů (X.509, CV, C-ITS, …)

Řízení digitálních podpisů (vzdálené, code-signing, QES, …)

CO SE MŮŽE STÁT

Výpadek služby způsobený nezabezpečeným a nedůvěryhodným certifikátem

Zvýšená pravděpodobnost narušení bezpečnosti způsobené nekonzistentními a zastaralými certifikáty

Ztráta reputace a poškození značky způsobené nedostupností veřejných zdrojů

Vynaložení značných finančních nákladů spojených s narovnáním situace, které lze investovat do jiných obchodních cílů společnosti.

Neobnovitelná ztráta identity vašich chytrých nebo IoT zařízení

Zvýšené riziko nesouladu se standardy a nařízeními platnými pro organizaci

Výpadek systému eRecept způsoben certifikátem

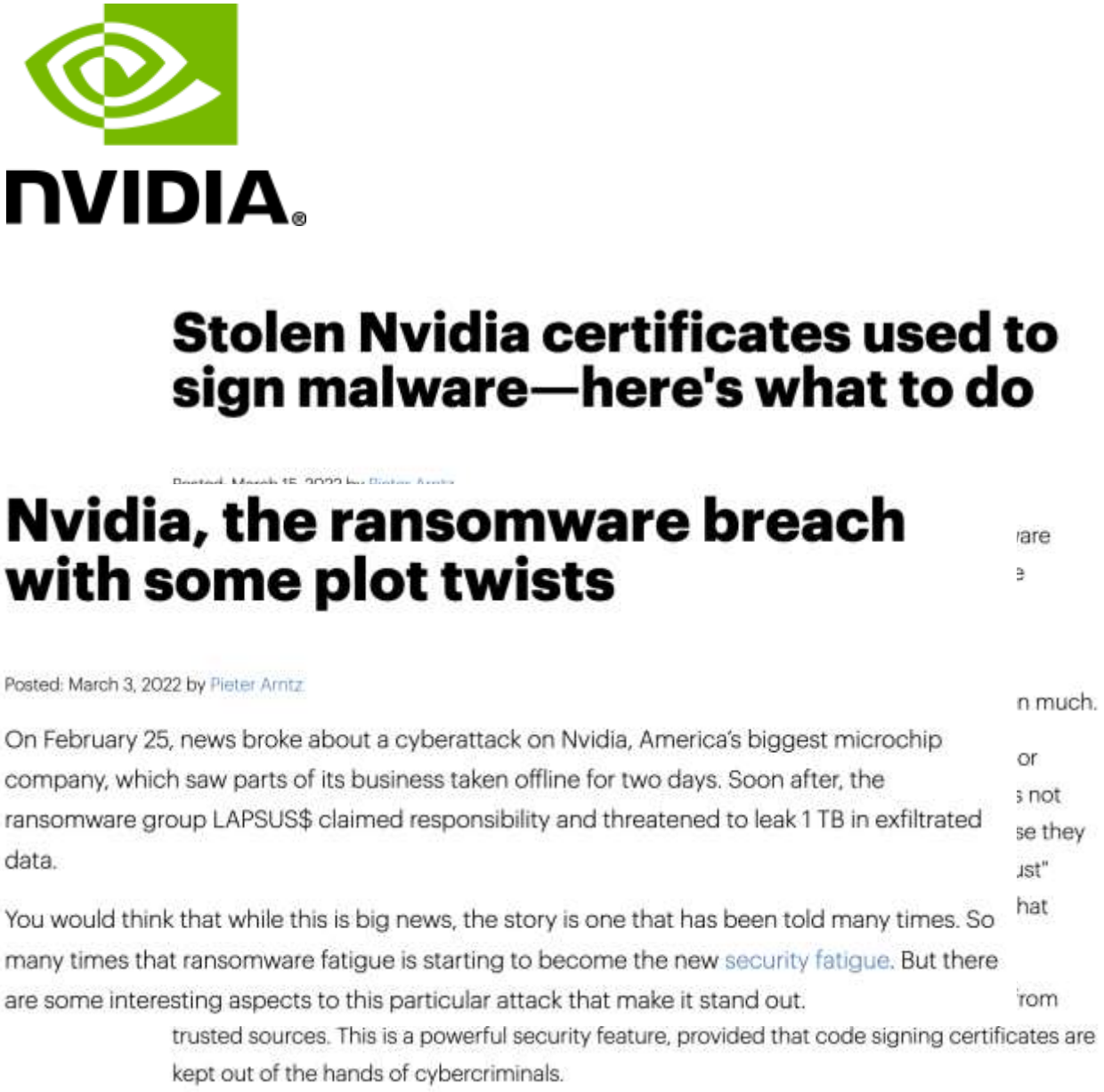
Inovace,Novinky / Napsal Dalibor Premus / 24 ledna, 2022 / Bezpečnost,Certificate,Certifikát,CLM,CÚER,CZERTAINLY,eRecept,Komunikace,Lifecycle,Management,PKI,Platforma,Podepisování,Řízení,SÚKL,Technologie,Výpadek

Systém elektronické preskripce, známý jako eRecept, se ve středu 19.1.2022 potýkal s technickými problémy, které způsobili jeho výpadek. Lékaři tak nemohli vydávat elektronické recepty a lékárníci zase léky, a to dokonce ani na dříve vydané a platné e-recepty. Ministr zdravotnictví Vlastimil Válek k výpadku systému eRecept na tiskové konferenci ve stejný den uvedl, že "Zkolaboval ...

Pokračovat ve čtení »

NEPLÁNOVANÉ VÝPADKY

- Způsobeno neplatným certifikátem
- Nefunkčnost systému po dobu několika hodin
- Není možné vydávat eRecepty
- Lidé si nemůžou vyzvednout léky
- Obrovský finanční a reputační dopad



Stolen Nvidia certificates used to sign malware—here's what to do

Nvidia, the ransomware breach with some plot twists

Posted: March 3, 2022 by Pieter Arntz

On February 25, news broke about a cyberattack on Nvidia, America's biggest microchip company, which saw parts of its business taken offline for two days. Soon after, the ransomware group LAPSUS$ claimed responsibility and threatened to leak 1 TB in exfiltrated data.

You would think that while this is big news, the story is one that has been told many times. So many times that ransomware fatigue is starting to become the new security fatigue. But there are some interesting aspects to this particular attack that make it stand out.

trusted sources. This is a powerful security feature, provided that code signing certificates are kept out of the hands of cybercriminals.

KOMPROMITACE IDENTITY

- Odcizené code-signing certifikáty včetně privátních klíčů (exspirované)
- Možnosti instalace driverů podepsaných exspirovaným certifikátem

DST Root CA X3 Expiration (September 2021)

Last updated: Sep 30, 2021 | See all Documentation

> ***Update September 30, 2021*** *As planned, the DST Root CA X3 cross-sign has expired, and we're now using our own ISRG Root X1 for trust on almost all devices. For more details about the plan, keep reading! We have also updated our Production Chain Changes thread on our community forum - our team and community are here and ready to help with any questions you may have about this expiration.*

On September 30 2021, there will be a small change in how older browsers and devices trust Let's Encrypt certificates. If you run a typical website, you won't notice a difference - the vast majority of your visitors will still accept your Let's Encrypt certificate. If you provide an API or have to support IoT devices, you might have to pay a little more attention to the change.

NESOULAD

- Včasná notifikace a upozornění o exspiraci certifikační autority
- Společnosti nereagovaly na update certifikační autority v systémech
- Způsobené výpadky
- Nesoulad a auditní nálezy spojené s procesy souvisejícími s PKI a řízením kryptografických klíčů
- Zvýšené náklady na obnovu

Supply chain attacks are not common and the SolarWinds Supply-Chain Attack is one of the most potentially damaging attacks we've seen in recent memory. Of course, as it is an evolving situation, we will likely know more as the days progress, but this is what we know as of now.

On December 8 FireEye announced that it had been hacked by a nation-state and since that announcement they've been incredibly transparent, publishing information about the breach and what they've learned about it in their investigation.

SolarWinds Breach

On December 13 Chris Bing of Reuters broke the story that the US Treasury Department has been compromised by a sophisticated adversary. Shortly after, Ellen Nakashima of the Washington Post confirmed with background sources that the US Treasury breach was perpetrated by the same group that targeted FireEye, that SolarWinds was involved in both breaches, and that it was perpetrated by threat group APT29 (Cozy Bear/Russian SVR).

SUPPLY CHAIN BEZPEČNOST

- Sunburst backdoor vložen do kódu během vývoje produktu
- Software update proces kompromitován
- Nepodepsaný kód vývojářů
- Napadeno více než 18.000 zákazníků včetně vládních organizací
- Obrovský finanční a reputační dopad

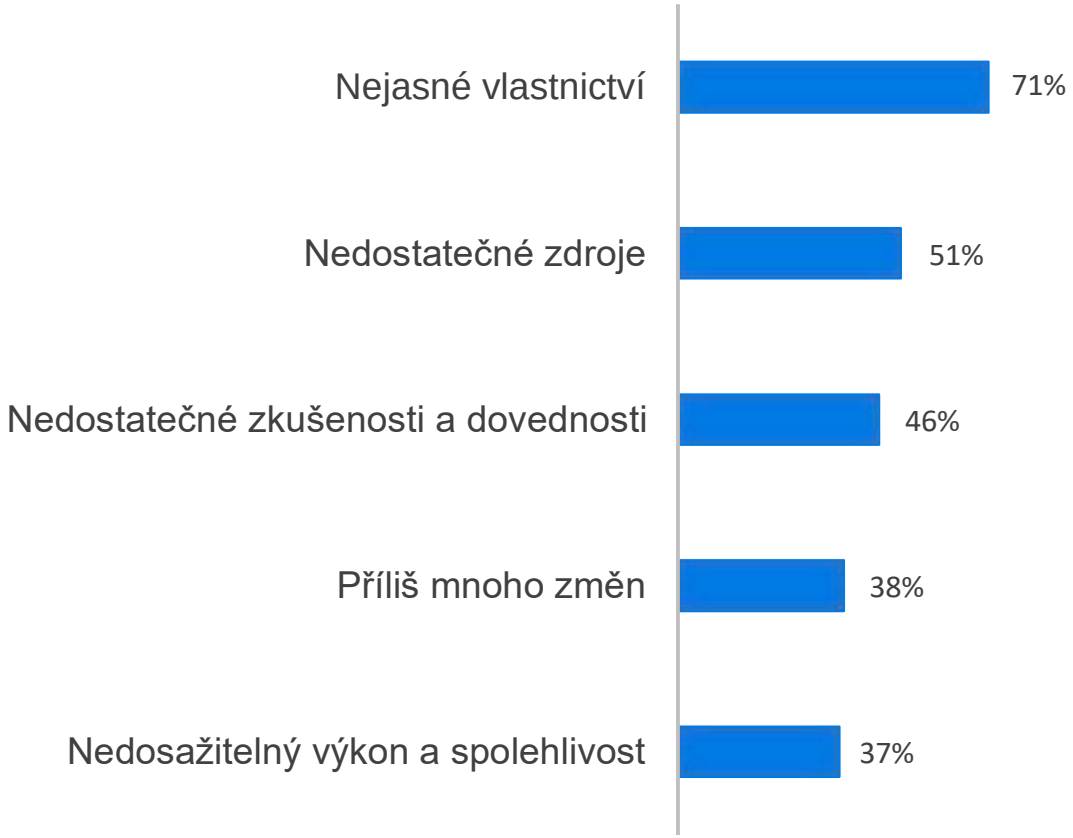
VÝZVY PRO SPOLEČNOSTI

50-80%
aplikací průměrně využívá certifikáty

50%
Společností nemá dostatek personálu dedikovaného pro PKI a šifrování

3,3 hod.
je průměrná doba zotavení se z výpadku

73%
organizací zaznamenalo neplánovaný výpadek kvůli nesprávně řízeným certifikátům



- 2021 Global PKI and IoT Trends Study
- 2022 State of Machine Identity Management

EXISTUJE ŘEŠENÍ?

- PKI se stává nedílnou a kritickou součástí systémů a služeb
- Vzniká potřeba automatizovat procesy spojené s řízením životního cyklu důvěryhodných služeb

INVESTICE A BUDOVÁNÍ

PŘEHLED A POVĚDOMÍ

AGILITA A AUTOMATIZACE

INVESTICE A BUDOVÁNÍ

Infrastruktura veřejného klíče

Řízení identit a přístupů (včetně privilegovaného)

Podepisování zdrojových kódů (a nejenom kódu)

Řízení životního cyklu digitálních certifikátů

Správci hesel a jiných sensitivních informací (pro přístup k systému)

Hardwarové moduly (HSM)

Řízení kryptografických klíčů

Rozšiřování vzdělání a zkušeností (hands-on)

PŘEHLED A POVĚDOMÍ

Přehled o certifikátech a kryptografických klíčích

Konzistence dat

Aplikované regulace, standardy, normy

Sledování změn stavu v čase

Periodické získávání informací o nově vydaných certifikátech

Skenování infrastruktury

Zjišťování self-signed certifikátů a neschválených autorit

Implementace strukturovaného procesu řízení

AGILITA A AUTOMATIZACE

Reakce na potenciální hrozby (například kompromitace)

Výměna kryptografických klíčů a změna algoritmů

Změna důvěryhodných certifikačních autorit

Automatizace výměny digitálních certifikátů v koncových systémech (včetně kryptografických klíčů)

Integrace s nástroji pro sledování a exekuci automatizace

Použití standardních rozhraní a protokolů

Automatizace kontroly souladu s politikami

Řízení výjimečných situací

3Key Company s.r.o.
Dalibor Premus
dalibor.premus@3key.company