Nový zákon o kybernetické bezpečnosti prakticky

Organizační a technická doporučení

GoodAccess

GUARDIANS CZ

Obsah

Nový ZoKB: evoluce či revoluce?

Závislost společnosti na informačních technologiích je dnes natolik silná, že bychom si bez nich její fungování dokázali už jen těžko představit. Energetika, vodní hospodářství, bankovnictví, doprava a mnoho dalších sektorů, tam všude hraje ICT zásadní roli.

Čím dál častěji se tak tyto služby kritické pro společnost stávají cílem kybernetických hrozeb, které navíc nabývají na sofistikovanosti. Ať už za účelem dosažení politických cílů, obohacení, nebo jen demonstrování síly.

Potřeba systematické ochrany je proto čím dál intenzivnější.

EVROPSKÁ SMĚRNICE NIS2

Evropská směrnice NIS2 (The Network and Information Security), reprezentovaná v České republice novým zákonem o kybernetické bezpečnosti (ZoKB), vstupuje na toto pole s razantními požadavky.

U nás by se nový ZoKB měl dotknout více než 6000 subjektů. Vzhledem k počtu dotčených subjektů, ale i rozsahu nových technických a organizačních opatření, je zřejmé, že dopad ZoKB bude zcela zásadní. Oproti GDPR se navíc jedná o natolik složitou problematiku, že k naplnění organizačních a technických požadavků zákona bude potřeba spolupráce advokátů, konzultantů a dodavatelů ICT.

Je tedy správný čas se na příchod nového zákona o kybernetické bezpečnosti připravit. Zavedení funkčního kyberbezpečnostního systému pro naplnění souladu se zákonem totiž může trvat měsíce, i roky. A bude spjato s velkými investičními a provozními náklady.

V tomto textu se snažíme přiblížit legislativní a organizační dopady ZoKB a představit možnosti technologie zero-trust při naplňování jeho požadavků.

2024: Zásadní rok pro kyberbezpečnost v Evropě

Pro Evropskou unii není téma boje proti kybernetickým rizikům nové. Už v roce 2016 vydala směrnici NIS za účelem standardizovat ochranu těch nejcitlivějších odvětví.

KOMPLEXNĚJŠÍ REGULACE

S rokem 2023 pak přichází její následovnice – NIS2, která si klade za cíl vytvořit vysoký společný standard kyberbezpečnosti napříč Unií. Oproti své starší sestře ale NIS2 představuje výrazně širší a komplexnější regulaci. Nařizuje totiž nejen ochranu všech systémů důležitých pro společnost, požaduje zabezpečit všechny systémy, které s poskytováním služeb důležitých pro společnost souvisí.

NOVÝ ZoKB

Do legislativy evropských států se směrnice promítne prostřednictvím národních úprav. V České republice se jedná o již zmíněný nový zákon o kybernetické bezpečnosti (ZoKB), který připravuje Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Ten představuje již konkrétní, pro povinné subjekty závazný předpis se specifickými ustanoveními pro český kontext a potřeby. V platnost by měl vejít do konce roku 2024.

Firmy či organizace, které spadnou do jeho působnosti, budou muset implementovat požadovaná bezpečnostní opatření ve formě **nasazení nových technologií a implementace bezpečnostních procesů.** Těch je celá řada a dotknou se velkého počtu subjektů z různých, dříve neregulovaných odvětví.

Regulováno bude více než 6000 českých firem a organizací s tím, že mnohé z nich budou muset požadavky zákona přenést smluvně i na své dodavatele.

Dojde tak k dramatickému navýšení počtu povinných subjektů, které nový ZoKB pojmenovává jako poskytovatele regulované služby. Ti budou rozděleni do 18 odvětví (např. digitální infrastruktura a služby, energetika, veřejná správa). Pro představu lze nahlédnout například do infografiky, kterou najdete na stránkách NÚKIBu.

ENERGETIKA
DOPRAVA
BANKOVNICTVÍ
ZDRAVOTNICTVÍ
INFRASTRUKTURA FIN. TRHŮ
DIGITÁLNÍ INFRASTRUKTURA
PITNÁ VODA
ODPADNÍ VODA
DIGITÁLNÍ INFRASTRUKTURA
POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB
VEŘEJNÁ SPRÁVA
VESMÍR
POŠTOVNÍ SLUŽBY
ODPADNÍ HOSPODÁŘSTVÍ
CHEMICKÝ PRŮMYSL
POTRAVINÁŘSTVÍ
VÝROBA
POSKYTOVATELÉ DIGI SLUŽEB
VÝZKUM
JINÉ

Jaké změny nový ZoKB přináší?

Jak už jsme naznačili, ZoKB přinese celou řadu zásadních změn. Obecně lze dopady nového zákona shrnout do pěti oblastí:

Větší rozsah

Nový ZoKB se dotkne více odvětví a služeb, včetně poskytovatelů veřejných elektronických komunikačních sítí a služeb, digitálních služeb (sociální sítě, poskytovatelé služeb datových center), nakládání s odpady a dalších (viz výše zmíněná infografika od NÚKIB).

Přísnější požadavky

Nový ZoKB zavádí řadu technických a organizačních opatření. Jsou mezi nimi například zabezpečení dodavatelského řetězce, kontinuity podnikání, krizového managementu, školení v kybernetické bezpečnosti, nasazení politik řízení přístupu, použití MFA nebo metod neustálé autentizace a další.

Změny sankcí

Nový ZoKB přináší změnu v sankcích, jednak navyšuje horní hranice finančních sankcí, ale zavádí i tzv. nefinanční sankce.

Posílený dohled

Dojde k posílení dohledu, povinnosti hlášení incidentů a uložení vysokých pokut při nenaplnění souladu se zákonem. Vedení dotčených subjektů může být nyní také přímo odpovědné za porušení právních předpisů.

Spolupráce v rámci EU

Jako transpozice NIS2 do národní legislativy ZoKB stanoví postupy pro sdílení informací/zkušeností napříč EU a pro koordinaci v případě velkých útoků.

Režimy povinností

Nová regulace dělí požadavky na bezpečnostní opatření do dvou režimů – vyšší režim povinností (přísnější) a nižší režim povinností.

REŽIMY

Poskytovatel regulované služby v režimu vyšších povinností (essential)

— sem spadají zpravidla nejkritičtější typy regulovaných služeb. Jedná se například o firmy z energetického průmyslu, dopravy, bankovnictví, veřejné správy atd.

Poskytovatel regulované služby v režimu nižších povinností (important)

— spadají sem zpravidla střední a velké firmy z oborů jako poštovní služby, potravinářství, chemický průmysl a další.

Lepší přehled o rozdělení na základní a důležité subjekty najdete na stránkách NÚKIBu. Jedná se o verzi platnou k 16. srpnu 2022, která ve finální podobě pravděpodobně dozná dílčích změn.

Jak poznám, že se nový ZoKB týká i mojí firmy či organizace?

Primární způsob stanovení, jestli soukromá nebo veřejná organizace spadá pod regulaci ZoKB, je současné naplnění dvou požadavků. Konkrétně je potřeba si odpovědět na dvě otázky:

Spadá obor mé činnosti do regulace?

Nový ZoKB a případně jeho prováděcí právní předpisy stanovují regulované služby a kritéria pro stanovení režimu regulace.

Je má firma či organizace dostatečně velká?

ZoKB se dotkne především středních a velkých podniků a organizací. Kritériem je zaměstnávat 50 a více zaměstnanců, nebo dosahovat ročního obratu nebo bilanční sumy roční rozvahy alespoň 10 milionů EUR.

Zjištění, zda splňuji druhou podmínku může být trochu komplikovanější, protože je nutné posuzovat i vztah k tzv. propojeným podnikům.

Pokud organizace spadá pod novou regulaci, je třeba si navíc odpovědět na otázku, jaké povinnosti je třeba plnit. Režim povinností (režim regulace), tedy zda spadá vaše firma do režimu vyšších povinností, nebo nižších povinností, je zpravidla definován pomocí kritérií uvedených v definici regulovaných služeb.

Současné znění těchto definic najdeme v návrhu vyhlášky o regulovaných službách **zde** (dokument Návrh prováděcích předpisů).

PORTÁL NÚKIB

Registrace na Portálu NÚKIB

Po naplnění kritérií je potřeba provést tzv. registraci na Portálu NÚKIB, jejímž smyslem je informovat regulátora, že subjekt naplňuje stanovená kritéria a spadá pod regulaci.

Dle současného návrhu by tak mělo být učiněno do 90 dnů od uvedení nového ZoKB v platnost, nebo od doby, kdy regulovaný subjekt překročí velikostní kritéria. Může ale také nastat situace, kdy sám NÚKIB vyhodnotí organizaci jako předmět regulace.

Kdo je v organizaci zodpovědný za NIS2/ZoKB a jaké hrozí sankce?

Regulované subjekty by měly mít zaměstnance, nebo dodavatele, kteří budou zajišťovat takzvané bezpečnostní role. Budou řídit a rozvíjet kybernetickou bezpečnost, dohlížet na její stav, navrhovat a implementovat bezpečnostní opatření a komunikovat kybernetickou bezpečnost s vedením.

Za to, že se tak stane, stejně jako za vyčlenění zdrojů na kyberbezpečnost, integraci bezpečnostních principů do všech procesů a za další, přitom bude odpovědný vrcholový management. Nový ZoKB tedy vyžaduje, aby se vrcholový management aktivně podílel na řízení kyberbezpečnosti, a stanovuje sankce v případě, že se tak nebude dít.

SANKCE

Horní hranice sankcí jsou nastaveny ve výši 2 % obratu v případě vyššího režimu povinností a 1,4 % v případě nižšího režimu povinností. Kromě finančních dopadů ale může nedodržování povinností vést i k pozastavení výkonu řídící funkce statutárního orgánu organizace osobě nebo k odebrání kyberbezpečnostních certifikací.

Do kdy musím mít vše připravené?

Dle současného návrhu budou mít poskytovatelé regulovaných služeb **rok na zavedení technických a organizačních opatření,** tedy na zajištění souladu s novým ZoKB.

S přípravou na nový zákon se však vyplatí neotálet zejména ze dvou důvodů.

POŽADAVKY

Zákon uvede v platnost řadu povinností a technických požadavků. Ty nemusí být jednoduché v prostředí větší, ale i středně velké firmy v požadovaném čase implementovat. Zvláště, pokud subjekt doposud kybernetickou bezpečnost komplexněji neřešil.

IMPLEMENTACE

S implementací navíc mohou být spojeny velké investiční a provozní náklady. Na ty je třeba vyčlenit zdroje, naplánovat je, a také najít, případně proškolit experty, kteří se budou o kybernetickou bezpečnost starat.

Samotný NÚKIB uvádí, že zavedení funkčního procesu řízení kybernetické bezpečnosti v organizaci může být otázka několika měsíců až let. Obzvláště, pokud se jedná o organizace spadající do režimu vyšších povinností.

Plnění bezpečnostních opatření

S novým ZoKB souvisí i další předpisy. Ty, které nás zajímají, pokud jde o bezpečnostní opatření, jsou dvě samostatné vyhlášky upřesňující požadavky pro jednotlivé režimy regulace (vyšší a nižší povinnosti).

V níže uvedené tabulce naleznete přehled požadavků na bezpečnostní opatření, kde srovnáváme požadavky na organizační a technická opatření u režimu vyšších a nižších povinností. Návrh jejich znění najdeme **zde**.

Organizační opatření	
Vyhláška pro režim vyšších povinností	**Vyhláška pro režim nižších povinností**
Systém řízení bezpečnosti informací	Systém řízení bezpečnosti informací
Povinnosti vrcholného vedení	
Bezpečnostní role	Bezpečnost lidských zdrojů
Řízení bezpečnostní politiky a dokumentace	*požadováno přes přílohu*
Řízení aktiv	
Řízení rizik	
Řízení dodavatelů	*požadováno přes přílohu*
Bezpečnost lidských zdrojů	*požadováno přes přílohu*
Řízení změn	-
Akvizice, vývoj a údržba	-
Řízení přístupu	
Zvládání kybernetických bezpečnostních událostí a incidentů	Řešení kybernetických bezpečnostních incidentů + stanovení významnosti incidentů
Řízení kontinuity činností	Řízení kontinuity činností
Audit kybernetické bezpečnosti	-

Tabulka 1: Srovnání organizačních opatření

Technická opatření	
Vyhláška pro režim vyšších povinností	**Vyhláška pro režim nižších povinností**
Fyzická bezpečnost	-
Bezpečnost komunikačních sítí	Bezpečnost komunikačních sítí
Správa a ověřování identit	-
Řízení přístupových oprávnění	Řízení identit a jejich oprávnění
Detekce kybernetických bezpečnostních událostí	Detekce a zaznamenávání kybernetických bezpečnostních událostí
Zaznamenávání bezpečnostních a relevantních provozních událostí	
Vyhodnocování kybernetických bezpečnostních událostí	-
Aplikační bezpečnost	Aplikační bezpečnost
Kryptografické algoritmy	Kryptografické algoritmy
Zajišťování dostupnosti regulované služby	-
Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv	-

Tabulka 2: Srovnání technických opatření

Kdo pomůže s implementací bezpečnostních opatření?

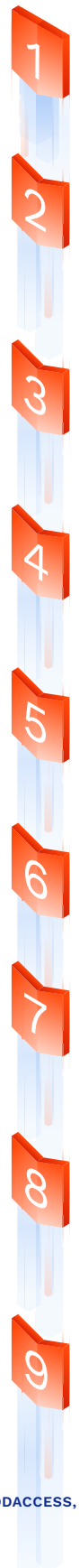
Zatímco organizace spadající do vyššího režimu regulace budou muset mít určeny tzv. bezpečnostní role (manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti a auditora kybernetické bezpečnosti), na organizace v nižším režimu regulace je kladen požadavek určit si „odpovědnou osobu za kybernetickou bezpečnost, která odpovídá za řízení a rozvoj kybernetické bezpečnosti, dohled nad stavem kybernetické bezpečnosti a komunikaci v oblasti kybernetické bezpečnosti s vrcholným vedením". V podstatě lze říci, že jde o roli manažera kybernetické bezpečnosti.

Ve všech případech je možné, aby tyto role zajišťovali jak vlastní zaměstnanci, tak dodavatelé v rámci outsourcingu.

Prakticky, jestliže organizace s implementací požadavků nového ZoKB začíná, bude potřebovat právě manažera kybernetické bezpečnosti, který by měl implementaci bezpečnostních opatření zajišťovat. Zpravidla na to ale nebývá sám, neboť víme, že technologie a jejich kybernetická bezpečnost jsou natolik komplexní, že se neobejdeme bez dalších expertů. A to nejen z oblastí jako jsou ICT, OT, ale i z oblastí jako je právo, audit, personalistika atp.

Jak by měl manažer kybernetické bezpečnosti postupovat

Zjednodušeně lze říci, že by manažer kybernetické bezpečnosti měl projít několika kroky:



1. Porozumí kontextu organizace a jejím obchodním cílům.
2. Pomůže se stanovením přehledu všech aktiv organizace, zjistí hodnoty aktiv a jejich souvislost s poskytováním regulovaných služeb organizace.
3. Zmapuje současný stav řízení kybernetické bezpečnosti organizace.
4. Zajistí proces řízení rizik a pomůže s identifikací a hodnocením rizik s ohledem na typ organizace, ideálně s podporou dat, které jsou dostupné v MITRE ATT&CK.
5. S ohledem na rizika sestaví plán zvládání rizik, prohlášení o aplikovatelnosti (přehled bezpečnostních opatření).
6. V návaznosti na předchozí kroky pomůže sestavit bezpečnostní strategii kybernetické bezpečnosti.
7. Sestaví projekt zavádění jednotlivých bezpečnostních opatření.
8. U vyššího režimu regulace, společně s architektem kybernetické bezpečnosti, definuje cílovou bezpečnostní architekturu organizace.
9. Společně pracuje na zavádění a testování bezpečnostních procesů (např. incident management, řízení přístupů atd.).

10 Podporuje organizaci při výběru vhodných technologických partnerů, dodavatelů bezpečnostních řešení (end-point protection, ZTNA, log management, SIEM/SOAR atd.).

11 Komunikuje s NÚKIB a příslušným CERT týmem ve věcech regulace.

12 Pomáhá zajišťovat kyberbezpečnostní školení.

13 Reportuje a zodpovídá se vedení organizace.

Zajišťování kybernetické bezpečnosti je pro organizace nikdy nekončící proces. Z hlediska cash-flow jsou největší výdaje na začátku projektu, tedy v době, kdy organizace implementuje nové procesy, pořizuje a implementuje nové technologie. Jakmile ale organizace v oblasti kybernetické bezpečnosti “dospívá”, dá se očekávat, že se náklady mohou snižovat.

Vybrané technologie pro naplnění požadavků ZoKB

Nová kyberbezpečnostní legislativa klade na regulované subjekty řadu požadavků na zavedení nových technologií. Lepší představu podává schéma č. 1, kde jsou zobrazeny technologie nutné pro zajištění souladu se zákonem.

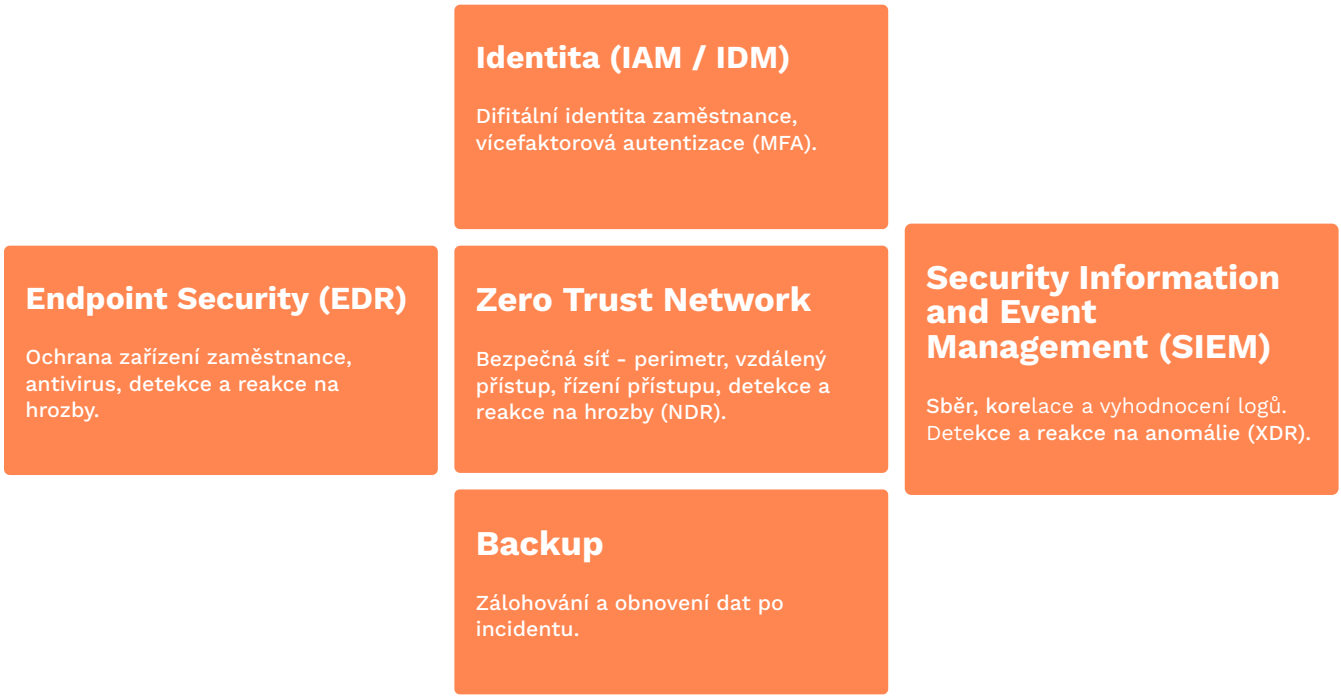


Schéma 1: Vybrané technologie pro naplnění požadavků ZoKB

K daným technologiím je možné ještě přidat služby MSSP (Managed security services provider). Takový subjekt se může jako subdodavatel starat o analýzu rizik, ISMS, nastavovat procesy, nebo zprostředkovávat služby manažera kybernetické bezpečnosti v rámci outsourcingu.

Mezi základy kybernetické ochrany, které výslovně zmiňuje i samotná směrnice NIS2, patří zavedení principů nulové důvěry (zero trust). V následujícím textu si představíme principy zero trust a jakým způsobem je lze v organizaci zavést, aby byly splněny požadavky ZoKB.

Co je to zero trust

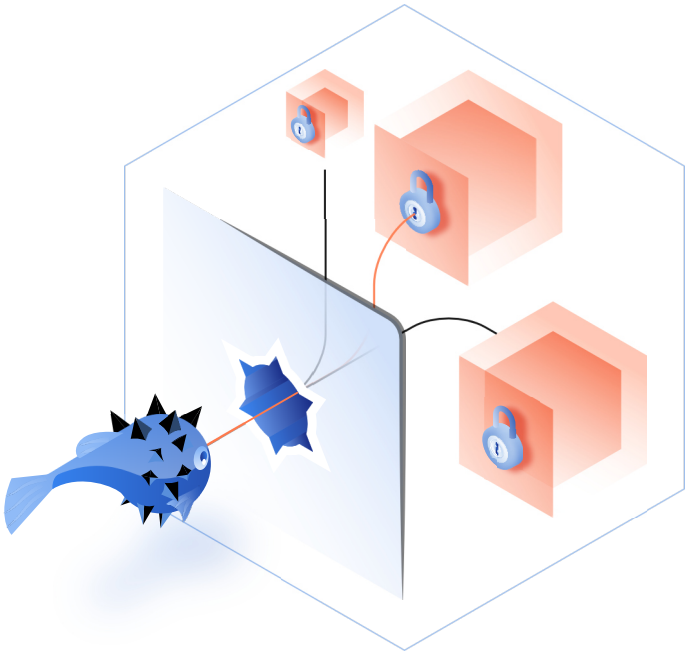
Zero trust je model bezpečnosti, který si klade za cíl snížit kybernetická rizika a eliminovat zranitelnosti. Fráze „nulová důvěra" odkazuje na praxi, kdy se každá část podnikové infrastruktury považuje za potenciální hrozbu. Jinými slovy, veškerý síťový provoz je potenciálně zákeřný a nelze mu důvěřovat.

Každý uživatel, zařízení a síťové připojení proto musí být ověřeno a validováno před tím, než je mu udělen přístup k aplikacím a datům.

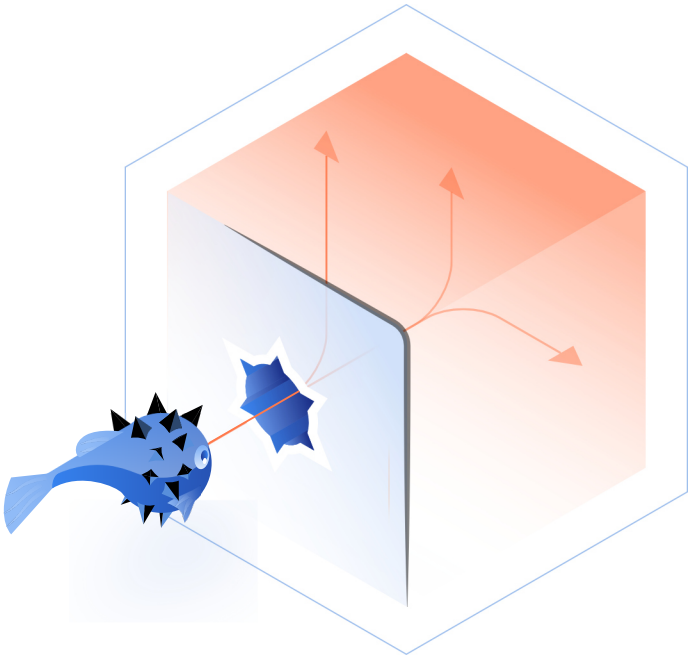
Tento model odpovídá na výzvy moderní bezpečnosti, kdy neexistuje tradiční hranice sítě. ICT zdroje se mohou nacházet v lokálních sítích, v cloudu nebo kombinovaně (hybridně) a zaměstnanci se k nim mohou připojovat z kteréhokoliv místa. Nasazením zero trust principů lze zlepšit celkovou připravenost organizace na kybernetické hrozby, snížit riziko bezpečnostních incidentů, neoprávněného přístupu a nežádoucího pohybu v IT infrastruktuře.

Řešení implementující principy zero trust budou pro naplnění požadavků nového ZoKB zásadní. Nejsou ale jedinými. Namátkou lze zmínit potřebu mít EDR řešení (Endpoint detection and response), správu identit, zálohovací technologie a další.

V následujícím textu blíže představíme konkrétní zero trust řešení GoodAccess a technické požadavky zákona, které lze s jeho pomocí naplnit.



Zero trust model bezpečnosti



Tradiční model bezpečnosti

Zero trust architektura v GoodAccess

GoodAccess je český SaaS nástroj, díky kterému lze rychle nasadit zero trust principy do bezpečnostní architektury organizace, a to bez významnějších zásahů do stávající infrastruktury. Firmy a organizace tak mohou jednoduše zabezpečit přístup k firemním systémům, sítím a datům odkudkoliv, kdykoliv.

Zero trust platforma GoodAccess agreguje více různých technologií. Pro snadnější porozumění lze využít analogie s fyzickým zabezpečením vysoce důležitých budov, jako jsou ministerstva, průmyslové provozy nebo kanceláře.

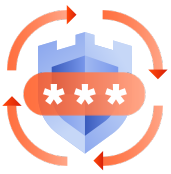
V takovéto analogii budova představuje síť s řadou ochranných prvků. Pojďme se tedy na klíčové prvky konceptu zero trust touto optikou podívat:

Device posture check

Ve fyzickém světě prochází zaměstnanec při vstupu do office budovy ochranným rámem, aby bylo zamezeno vstupu se zbraní nebo s jiným nežádoucím předmětem. Ve virtuálním světě takovouto detekci zajišťuje tzv. device posture check. Tato funkce při vstupu uživatelského zařízení (počítače, chytré telefony, tablety atd.) do sítě kontroluje, zda je bezpečné dle nastavených politik. Tedy například zda má aktualizovaný a zapnutý antivirus, zda je systém chráněn firewallem, zda je aktualizovaný operační systém, zda je šifrován disk, zda je zařízení chráněno biometrií apod.

Identity management (MFA)

Po průchodu bezpečnostním rámem člověk musí prokázat svoji totožnost. Předloží zaměstnaneckou kartu na recepci ke kontrole (případně na turniketu) a je vpuštěn dovnitř pouze v případě, že jeho identita odpovídá té v databázi. Ve světě zero trust také dochází k takovému ověření s tím, že se obvykle nestačí jen prokázat správnými přístupovými údaji, ale též dalšími prvky, jako je například biometrie nebo přihlášení se ze schváleného uživatelského zařízení.

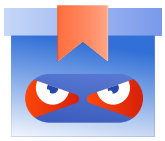


Access control

Pokud zaměstnanec projde kontrolou vstupu, obvykle nemá možnost se pohybovat po budově zcela volně. Má přístup jen na ta patra a do těch místností, které se týkají jeho práce. Koncept zero trust k bezpečnosti přistupuje stejně. Pomocí segmentace stanovuje, ke kterým systémům má kdo přístup. Minimalizuje se tak riziko zneužití dat a v případě incidentu lze lépe vyšetřit jeho příčinu. Fyzické a digitální zabezpečení lze dokonce propojit (GoodAccess toho dosahuje díky integraci s partnerem ProID, který dokáže pomoci s fyzickými přístupovými kartami i MFA na síťové/aplikační vrstvě).

Access logs

I ve fyzickém světě je pohyb po budově zaznamenáván. Pokud například člověk jde do skladu, nebo si “bookne” zasedačku, musí se obvykle podepsat na nějakou listinu. Pokud si pak například někdo odnese komunikační zařízení typu Jabra z meetingovky, lze snadno dohledat, kdo tam v daný čas byl a situaci prošetřit. Podobné je to ve virtuálním světě. GoodAccess schraňuje logy o přístupech do systémů, což se hodí pro předcházení, ale i investigaci incidentů. Přístupy do kritických systémů jsou navíc logovány na síťové vrstvě. Lze tak zastřešit kontrolu nad celým perimetrem a zákazník není závislý na schopnostech jednotlivých aplikací.



Threat detection and response

Stejně jako kamery sledují aktivity a chování lidí v různých částech budovy, jsou i součástí zero trust technologie pro monitorování „pohybu” a chování zaměstnanců na síti. Obvykle díky integraci s NDR nebo SIEM řešením. Díky tomu pak lze mít pod kontrolou například dodržování firemních politik, ale i identifikovat trendy a neobvyklé chování. S GoodAccess lze zajistit, že jediná cesta k danému systému vede přes GoodAccess gateway (lokální nebo cloudovou). Tím lze v případě detekované hrozby automaticky zamezit přístupu konkrétnímu zaměstnanci nebo zařízení a zastavit útok v jeho rané fázi.

Nasazení GoodAccess

S nasazením řešení pro zero trust bývají spjaty nejrůznější překážky, jako nekompatibilita aplikací se zero trust principy, složitost správy řešení, omezené zkušenosti a znalosti, nedostatečná flexibilita, nebo finanční náklady.

Největším problémem je obvykle nehomogenní infrastruktura. Tedy infrastruktura založená na více dodavatelích síťových prvků, rozprostírající se přes více cloudových prostředí a poboček, kde aplikace nejsou kompatibilní s SSO a MFA. V takové infrastruktuře je velmi těžké zajistit bezpečný přístup zaměstnanců, zvláště pokud používají vlastní zařízení, nebo přístupy sub-dodavatelů k důležitým IT zdrojům.

Podívejme se na to, jak cloudové řešení GoodAccess uvedené překážky eliminuje:

Pracuje na síťové vrstvě

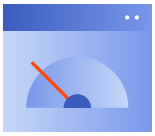
Díky tomu umožňuje poskytovat autentizovaný přístup i k starším aplikacím a systémům, které často nejsou kompatibilní s jednotným přihlašováním (SSO) a multifaktorovou autentizací (MFA). GoodAccess lze navíc jednoduše integrovat se stávající ICT infrastrukturou, ať už se jedná o poskytovatele identit (identity providers), síťový hardware (routery), nebo poskytovatele cloudových služeb (AWS, Google, Azure a další).

Přístup k systémům a datům odkudkoliv

GoodAccess je z uživatelského pohledu „one-click” aplikace. Je tedy jedno, zda zaměstnanec pracuje na Android, macOS, iOS, Windows nebo Linux zařízení. Má na něm nainstalovanou aplikaci (agenta) a po přihlášení přes multifaktorovou autentizaci, ověření identity a úspěšném device posture checku (ověření bezpečnosti zařízení) získá uživatel bezpečný, šifrovaný přístup k firemní zero trust síti.

Snadná správa chráněného prostředí

GoodAccess je navržen tak, aby pro jeho správu nebylo třeba hlubších IT znalostí. Administrátor pracuje ve webovém rozhraní, kde má své chráněné prostředí plně pod kontrolou. Může spravovat uživatelské účty a jejich práva, definovat chráněné systémy (včetně propojení na pobočky a cloudy), dohlížet na síťovou aktivitu a zabezpečení zařízení. V případě hrozby má možnost zařízení odstřihnout od sítě a incident investigovat.



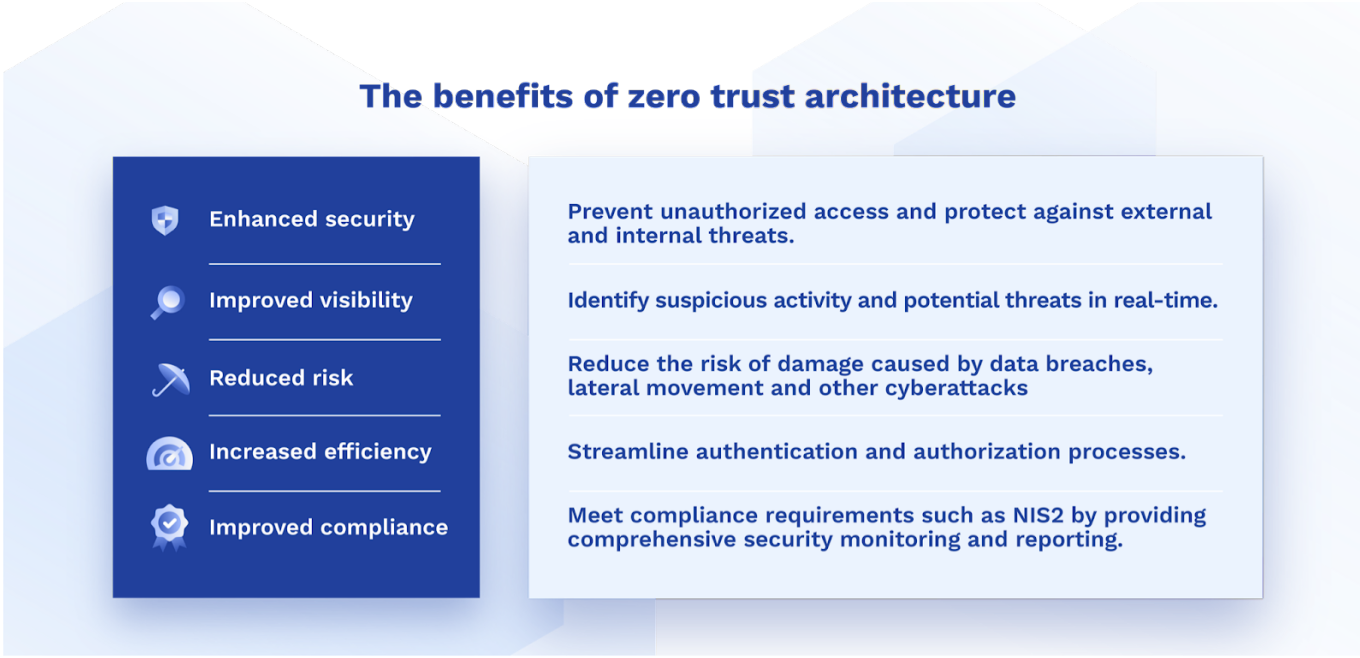
Automatizace a škálovatelnost

GoodAccess lze přímo integrovat s digitální identitou (Identity access management) a řadu rutinních úkolů spjatých se správou uživatelských identit a účtů automatizovat. HR oddělení tak například může v IAM nástroji spravovat uživatelské skupiny a jejich práva, přičemž nastavení se díky SSO nebo SCIM automaticky propíše do GoodAccess. Takováto synchronizace významně šetří čas a umožňuje rychleji reagovat na měnící se potřeby firmy. Eliminuje také bezpečnostní rizika spjatá s lidskou chybou při ručním přidávání/odebírání zaměstnanců a zařízení do chráněné sítě.

Vzhledem ke cloudové povaze GoodAccess je škálování otázkou několika kliknutí, o vše se stará dodavatel.

Nižší náklady

Provozování in-house zero trust řešení s sebou nese dodatečné náklady na infrastrukturu a údržbu systému. To může být pro firmu dodatečná zátěž spojená s updaty systému, ošetřováním zranitelností atd. Navíc je potřeba certifikovaného experta, který se o systém bude starat. V případě cloudového řešení se o vše stará dodavatel a náklady jsou díky subscription modelu jasně predikovatelné.



Obrázek 1: Výhody implementace zero trust řešení

Jak GoodAccess pomáhá s naplněním technických opatření ZoKB

Technické opatření	
Fyzická bezpečnost	Zde se jedná o bezpečnost ve fyzickém světě a technicko-procesní řešení. Náš partner ProID dokáže sjednotit identitu ve fyzickém i digitálním prostředí pomocí fyzických přístupových karet a HW tokenů.
Bezpečnost komunikačních sítí	GoodAccess zajišťuje autentizovaný síťový provoz, řízení přístupu na úrovni sítě, šifrování a bezpečný vzdálený přístup z jakéhokoliv zařízení zaměstnance. V rámci Zero Trust Perimetru (SDP) pak dochází k segmentaci sítě, definování kritických systémů jako síťových služeb, ke kterým neexistuje jiná síťová cesta, než přes perimetr. Dochází tak k izolování kritických systémů od veřejného internetu a dalšího neautentizovaného síťového provozu.
Správa a ověřování identit	GoodAccess se plně integruje s poskytovateli identity zaměstnanců (IAM/IDM) pomocí protokolů SSO, SAML a SCIM. Tím zajistíme vícefaktorovou autentizaci (MFA) nejen aplikační, ale i síťové vrstvy. Lze tak zajistit MFA i pro starší aplikace, které SSO/SAML nepodporují. GoodAccess lze použít i pro Priviledge Access Management (PAM) tak, že vytvoříme dočasnou (časově omezenou) přístupovou kartu pro administrátorský přístup ke konkrétnímu kritickému systému, která se po uplynutí času automaticky zneplatní a síťový přístup bude zrušen.
Řízení přístupových oprávnění	GoodAccess umožňuje centrálně řídit přístup k jednotlivým kritickým systémům (aktivům) na úrovni sítě, a to nezávisle na schopnostech kritické aplikace. V závislosti na povaze kritické aplikace může být v některých případech potřeba další řízení oprávnění a přístupů přímo uvnitř aplikace, a to už na aplikační úrovni.

Technické opatření	
Detekce kybernetických bezpečnostních událostí	Zde je potřeba kombinovat ochranu a detekci hrozeb na koncových zařízeních (EDR) s detekcí hrozeb na úrovni síťě. GoodAccess dokáže zajistit základní detekci v rámci platformy. V některých případech může být vhodné přidat nástroj pro pokročilou analýzů síťového provozu (NDR). GoodAccess integrovaný se SIEM pak dokáže na detekované hrozby okamžitě reagovat tak, že zablokuje síťový přístup uživatele/zařízení ke kritickému systému (aktivu). Zneplatnění přístupové karty může proběhnout ručně nebo automaticky, což je optimální pro úspěšné zastavení útoku v jeho rané fázi.
Zaznamenávání bezpečnostních a relevantních provozních událostí	GoodAccess zaznamenává bezpečnostní a relevantní provozní události na úrovni komunikační sítě a síťového perimetru. Poskytuje tak detailní přehled o jednotlivých přístupech do perimetru a v rámci sítě i ke konkrétním kritickým systémům (aktivům).
Vyhodnocování kybernetických bezpečnostních událostí	GoodAccess lze plně integrovat se SIEM. Umožňuje tak další zpracování záznamů, jako např. korelaci se záznamy z EDR a IAM pro účinnou detekci anomálií a hrozeb na všech úrovních.
Aplikační bezpečnost	GoodAccess chrání aplikace tak, že je izoluje od veřejného internetu a neautentizovaného provozu na síti. Zde je však potřeba navíc zajistit pravidelné skenování zranitelností, pravidelné aktualizace a penetrační testování.
Kryptografické algoritmy	Pokud zajistíme úplné nasazení GoodAccess, zajistíme bezpečný Zero Trust Perimetr a zamezíme přístupu ke kritickým systémům (aktivům) jinou cestou než po síti v rámci GoodAccess, pak je zajištěno šifrování veškeré komunikace na úrovni sítě. Pro účinnou ochranu doporučujeme vždy doplnit i o šifrování na aplikační vrstvě (SSL/TLS, end-to-end apod.).
Zajišťování dostupnosti regulované služby	Lze naplnit technicko-procesním zajištěním Zálohování, obnovení a redundance.
Zabezpečení průmyslových, řídících a obd. spec. technických aktiv	Kromě bezpečnosti fyzického přístupu lze GoodAccess dle popsaných principů použít i pro zabezpečení průmyslových, řídících a obd. spec. technických aktiv.

Závěrem

Zavedení nového zákona o kybernetické bezpečnosti staví před regulované firmy a organizace značné technické, organizační a právní výzvy. V tomto dokumentu jsme popsali klíčové oblasti pro naplnění zákona, které pomohou se v této problematice lépe zorientovat.

Je jisté, že naplnění souladu s novým zákonem o kybernetické bezpečnosti nebude vždy jednoduché. Zmapování potřeb firmy ve vztahu k novému ZoKB, vypracování strategie, zavedení nových technologií, přizpůsobení vnitřních politik a zavedení nových organizačních procesů, to vše bude vyžadovat čas, úsilí, a také finanční prostředky.

Proto je vhodné s přípravou neotálet a již nyní najít vhodné partnery, kteří s naplněním zákona pomohou. Technologická aliance GoodAccess společně s Guardians.cz, ProID a LogManager je v této oblasti silným partnerem, který u zákazníka umí požadavky nového ZoKB pokrýt.

Máte-li o danou problematiku zájem, neváhejte nás kontaktovat. Více informací na **nis2.goodaccess.com**.

Michal Čížek
CEO společnosti GoodAccess

P: **+420 605 264 263**
E: **michal@goodaccess.com**
W: **www.goodaccess.com**

DISCLAIMER

Upozornění

V ČR dosud není finální a platná verze nového ZoKB, ani jeho prováděcích právních předpisů. Proto může dojít k mírným změnám výše uvedených informací. Ty jsou aktuální ke dni 2.4.2024.