**Šest technologických trendů, které ovlivní bezpečnostní sektor v roce 2022**

***Rok 2021 utekl jako voda i, a proto je správný čas bilancovat, co nám přinesl, a zároveň se zamyslet nad výzvami a trendy, které ovlivní rok 2022. Odborníci společnosti Axis se z tohoto hlediska zabývají tím, co znají nejlépe, tedy oborem bezpečnostních technologií.***

Tyto předpovědi připravujeme již několik let a velmi často v nich v různých kontextech zmiňujeme pojem „důvěra“. V průběhu let jsme mluvili o důvěře ve využívání získaných dat nebo o důvěře v bezpečnost systémů či jednoduše o základní důvěře v to, že organizace dělají správné věci. Vidíme, jak je důležité sladit aktuální tempo technologických inovací s budováním důvěry ve využívání nových technologií.

Ze strany jednotlivců, organizací, ale i zákonodárců sílí volání po tom, aby se nové technologie vyvíjely, vyráběly a používaly způsobem, kterému můžeme plně důvěřovat. Pro společnost Axis to samozřejmě znamená pokračovat v práci na vizi inteligentnějšího a bezpečnějšího světa. Pohled do roku 2022 nám ukazuje, kolik zajímavých technologických trendů může být v krátké době spojeno s potřebou vybudovat důvěryhodný technologický ekosystém.

**Univerzální propojení v hybridních prostředích**

Pro koncového uživatele technologií – od spotřebitele používajícího svůj mobilní telefon až po bezpečnostní personál spravující dohledové systémy – se již technologická architektura používaná k poskytování služeb stala neviditelnou. Nezáleží na tom, zda zpracování a analytika probíhá přímo v zařízení, na místním serveru nebo ve vzdáleném datovém centru, protože je vše „propojeno“.

V loňském roce jsme uvedli, že se svět stane „horizontálním“ a bude se více využívat společná integrace cloudových, lokálních serverových a edge technologií, přičemž každá bude využívat své silné stránky v tzv. hybridních řešeních napříč těmito prostředími. To se nezmění ani v následujícím roce, ale je zřejmé, že otázka architektury je pro každého zákazníka jedinečná a musí zohledňovat i interní zdroje a politiky, jakož i další faktory (například místní, či mezinárodní předpisy). Jelikož se „propojení“ stalo standardem, jsme přesvědčeni, že většina dohledových řešení bude nakonec více či méně hybridní.

**Kybernetická bezpečnost se rodí ze zdravého skepticismu**

Ne vždy považujeme skepticismus za pozitivní vlastnost, ale v souvislosti s kybernetickou bezpečností je to rozhodně rozumné. Miliardy spojení, která dnes existují mezi zařízeními, sítěmi a datovými centry, způsobily, že koncept zabezpečení jakékoli organizace je zcela zastaralý. Bezpečnostní hradby, které jsme si vytvořili pro ochranu sítí, mají dnes množství různých děr, a proto byl zaveden nový přístup k bezpečnosti - tzv. [Zero Trust sítě](https://www.axis.com/blog/secure-insights/zero-trust-networks/%22%20%5Ct%20%22_blank).

Pokud se vám tento bod zdá povědomý, nemýlíte se. Zmiňovali jsme ho již v loňském příspěvku o technologických trendech. Zatímco před rokem jsme předpovídali rychlou akceleraci směrem k architekturám sítí s nulovou důvěrou, dnes už předpovídáme, že to bude standardní přístup. Svou roli zde sehrála také pandemie COVID-19, protože díky potřebě flexibilnější práce se mnohem víc zařízení připojuje na dálku s využitím veřejného internetu.

Přístup Zero Trust znamená, že se za výchozí stav považuje nulová důvěra, tedy že bezpečnostní profil každého zařízení i aplikace připojující se k síti je při každém připojení posuzován nezávisle, což má významný dopad také na sektor videodohledu.

Podepsaný firmware, pravidelné aktualizace, zabezpečené spouštění zařízení, šifrování dat a videa nebo zabezpečená identita se v zákaznických řešeních stanou nezbytnými faktory základní bezpečnostní hygieny.

**Ověření pravosti všeho**

Zatímco přístup Zero Trust se v rámci kybernetické bezpečnosti soustředí na ověřování pověření připojených zařízení a aplikací, základem důvěry u video dohledu je pravost videa. V důsledku možné manipulace s videozáznamem po jeho zachycení a stále sofistikovanějších způsobů, jak lze vytvářet a falšovat realisticky vypadající obraz, může být pravost videozáznamů často zpochybňována. Bude proto nezbytné, aby se videozáznam dal nezpochybnitelně označit za pravý.

Náš přístup spočívá v přidání digitálního podpisu do videa již v místě jeho zachycení (hash součet v každém jednom snímku videa), což by poskytlo jasný důkaz o tom, že video bylo pořízeno konkrétní kamerou a že s ním dále nebylo manipulováno.

Jedná se ovšem o problém celého odvětví bezpečnosti, a proto je nezbytné, aby se všichni jeho aktéři spojili s cílem vytvořit standard pro zajištění autenticity videozáznamů zachycených monitorovacími kamerami, ideálně na základě softwaru a iniciativ s otevřeným zdrojovým kódem.

**AI se stane etablovanou a akceptovanou (s příslušnými kontrolními mechanismy)**

Vypadá to, že nelze napsat příspěvek o technologických trendech bez zmínky o umělé inteligenci (AI). Mnozí by také mohli tvrdit, že AI již není trendem v pravém slova smyslu, protože tento džin byl již nadobro vypuštěn z láhve. Ve skutečnosti všichni denně využíváme nějaké služby založené na umělé inteligenci a hlubokém učení. Jsme přesvědčeni, že technologie jako taková by neměla být regulována, ale mohly by se regulovat případy jejího použití. Legislativa a regulace týkající se vývoje a používání technologií a aplikací založených na AI by měly být rozvíjeny na místní, regionální i mezinárodní úrovni. To by měla dodržovat každá organizace využívající umělou inteligenci.

Ačkoli v oblasti videodohledu vnímáme potenciál AI a hlubokého učení stále velmi pozitivně, rádi bychom podpořili takové iniciativy, které mají za cíl podpořit implementaci AI eticky a bez zaujatosti.

Bude to ještě důležitější, pokud se AI stane součástí každého aspektu videodohledu. Větší integrace umělé inteligence do nejzákladnějších úrovní technologie (systému na čipu (SoC)) s sebou přinese využívání AI ke zlepšení a optimalizaci všech aspektů videodohledu, od konfigurace kamer přes vylepšení kvality obrazu až po video analýzy.

**COVID-19 jako katalyzátor**

Dlouhodobý vliv dopadů COVID-19 se projevuje v různých oblastech. Pandemie byla již v minulosti katalyzátorem vývoje bezdotykových a nízkokontaktních technologií, z nichž mnohé se trvale integrovaly, stejně jako používání inteligentního videa pro zajištění dodržování sociálního odstupu a pokynů v oblasti veřejného zdraví. Pandemie vyústila také v problémy v dodavatelském řetězci a přinutila mnohé organizace zvážit způsob toho, jak vytvářejí a získávají klíčové komponenty pro své produkty.

„Propojená“ povaha všeho znamená, že globální nedostatek polovodičů způsobil významné problémy v mnoha odvětvích od spotřebitelských technologií až po automobilovou výrobu. Stále více organizací – mezi nimi i [Tesla](https://www.wired.com/story/why-tesla-designing-chips-train-self-driving-tech/%22%20%5Ct%20%22_blank), [Apple](https://www.bbc.com/news/technology-53142989%22%20%5Ct%20%22_blank) a [Volkswagen](https://www.eenewsautomotive.com/news/volkswagen-plans-own-chip-development%22%20%5Ct%20%22_blank) - veřejně vyjádřilo přání navrhovat si vlastní polovodičové systémy nebo systémy na čipu (SoC) (je potřeba zdůraznit, že navrhování SoC a jejich výroba jsou velmi odlišné činnosti). Tento zdánlivě nový trend v některých odvětvích je ale něco, co společnost Axis se systémem [ARTPEC](https://www.axis.com/newsroom/article/chip-quality-every-layer%22%20%5Ct%20%22_blank) dělá již léta a očekáváme, že navrhování vlastních SoC optimalizovaných pro konkrétní aplikace bude využívat stále více organizací v bezpečnostním sektoru i mimo něj.

**5G hledá své místo**

Někdo by mohl namítat, že je zbytečné zdůrazňovat 5G jako „trend“ v sektoru dohledu vzhledem k tomu, že je na pořadu dne již několik let. My však vidíme zásadní rozdíl mezi „hype“ a „trendem“. Podle odborníků ze společnosti Axis se nová technologie stává trendem teprve tehdy, když se začnou objevovat hodnotné případy jejího nasazení. Přestože si myslíme, že v případě 5G stojíme stále na startu, začíná se to měnit. Zatímco se velká část 5G soustředí na zlepšení výkonu sítí pro spotřebitelské aplikace, my vnímáme jako mnohem zajímavější a přesvědčivější případ nasazování této technologie ve vznikajících soukromých sítích.

Domníváme se, že soukromé 5G sítě ukazují skutečný potenciál pro řešení videodohledu ve velkých nebo více zákaznických lokalitách a mohly by přinést zvláštní výhody zejména z pohledu kybernetické bezpečnosti. Samozřejmě, když zákazníci vytvářejí privátní 5G sítě, je zapotřebí, aby se také videodohled mohl bez problémů integrovat, což představuje velký prostor pro všechny.

**Všechny trendy z pohledu udržitelnosti**

Udržitelnost již nelze považovat za trend. Musí být zakotvena ve všem, co děláme, tedy v tom, jak navrhujeme a vyrábíme produkty, i v tom, jak řídíme naše podnikání. Vše musí být v souladu se snižováním našeho vlivu na životní prostředí a fungováním etickým a důvěryhodným způsobem. Zkoumání trendů z pohledu kritérií udržitelnosti je stejně důležité jako jejich identifikace.

Rok 2022 bude nepochybně dalším fascinujícím rokem, který nebude bez výzev, ale přinese i významné příležitosti. Jako vždy na něj nahlížíme s optimismem.

***Johan Paulsson,*** *Axis Communications*