AXIS Camera Station 5

Průvodce posílením zabezpečení systému

Úvod

Úvod

Úvod

Univerzální a spolehlivý prvek, který dokáže zajistit 100% kybernetické zabezpečení jakéhokoli bezpečnostního systému a pracoviště. Jakkoli atraktivně tato slova znějí, žádný takový prvek neexistuje a pravděpodobně ani v dohledné době existovat nebude. Místo toho je třeba zkoumat riziko, které představují hrozby a zranitelnosti jedinečné pro danou organizaci, a pokud je riziko považováno za nepřijatelné, zavést řídicí mechanismy, které toto riziko zmírní. Dobře definované zásady a postupy zajišťují konzistentní komunikaci a uplatňování těchto řídicích mechanismů v celé organizaci a tvoří základ vyzrálého programu kybernetické bezpečnosti.

Doporučeným přístupem je pracovat podle standardizovaných rámců pro řízení bezpečnostních rizik IT, jako je ISO 27001, NIST CSF nebo jiné. Přestože může být tato úloha pro menší organizace náročná, je mnohem lepší definovat základní soubor zásad zabezpečení bezpečnosti a podpůrných procesů než nemít vůbec nic. Pokud se vaše organizace nachází teprve na začátku cesty ke kybernetické vyspělosti a má k dispozici omezené zdroje, doporučujeme prozkoumat *standard Critical Security Controls verze 8 Centra pro bezpečnost internetu (CIS).* CIS poskytuje seznam 18 bezpečnostních činností řízení, které jsou rozděleny do tří implementačních skupin a pomáhají organizacím rozvíjet a zdokonalovat program kybernetické bezpečnosti.

K narušení zabezpečení dochází v mnoha organizacích proto, že společnost nestanovila jasné zásady, pravidla a postupy, které by řídily používání a přístupová práva vlastních zaměstnanců. Používá vaše organizace zásady a procesy pro správu videa? Pokud ne, je načase, abyste si je začali definovat.

Účel

Tento dokument popisuje řadu zásad a postupů kybernetické bezpečnosti, které jsou užitečné pro zajištění bezpečného nasazení a údržby systémů . Ačkoli naše zásady nejsou přímo přiřazeny k rámci kybernetické bezpečnosti, vycházíme především ze standardu CIS Security Controls v8 se zvláštním zaměřením na následující prvky zabezpečení:

- *Prvek 1: Inventarizace a řízení podnikových aktiv*
- *Prvek 2: Inventarizace a řízení softwarových aktiv*
- *Prvek 3: Ochrana dat*
- *Prvek 4: Bezpečná konfigurace podnikových aktiv a softwaru*
- *Prvek 5: Správa účtů*
- *Prvek 6: Správa řízení přístupu*
- *Prvek 7: Nepřetržitá správa zranitelností*
- *Prvek 10: Obrana proti malwaru*

Naše doporučení se zaměřují na pomoc osobám zodpovědným za instalaci a integraci a koncovým uživatelům při zmírňování běžných rizik při nasazování a správě systémů .

Předpoklady

Předpokládá se, že chápete a dodržujete doporučení a postupy definované a popsané v *Průvodci posílením zabezpečení AXIS OS.* Tento dokument také odkazuje na několik běžných uživatelských rolí, které komunikují s video systémem. Namapujte tyto uživatelské role tak, aby odpovídaly vašim vlastním klasifikacím uživatelů a rolí. Jednotlivý uživatel může mít v závislosti na organizaci více rolí.

Definované role:

- **Osoba instalující systémy**: instaluje, nastavuje, opravuje, aktualizuje a downgraduje systémy.
- **Správce sítě**: spravuje síťovou infrastrukturu, konektivitu koncových uzlů, síťové servery a zdroje a také ochranu sítě.
- **Správce video systému**: definuje a spravuje video systém s cílem zabezpečit jeho používání, výkon a uživatelská oprávnění.

Úvod

- **Technik video systému**: z pověření správce video systému monitoruje, nastavuje systém a řeší problémy s komponentami, aby zajistil funkčnost systému.
- **Uživatelé**: osoby, které používají klienta za účelem přístupu k živému a nahranému videu a které jsou obvykle odpovědné za zajištění fyzické ochrany organizace.

Zásady zabezpečení systému

Fyzické zabezpečení

Zásady fyzické ochrany

Servery, zařízení, síťové vybavení a kabely jsou fyzické objekty, které mohou být narušeny, sabotovány nebo odcizeny. Hostitelský počítač se softwarem serveru a důležitá síťová zařízení (routery, přepínače atd.) je třeba umístit do prostředí s fyzicky a logicky omezeným přístupem. Kamery a další připojená zařízení je třeba instalovat na těžko přístupná místa a vybavit je modely nebo kryty odolnými proti vandalismu. Je třeba dbát na ochranu kabelů ve stěnách nebo kabelovodech, protože se zde existuje riziko neoprávněné manipulace a sabotáže.

Doporučené zásady a postupy
Definujte jednotlivce nebo organizační jednotku odpovědnou za vizuální audit fyzické ochrany serverů VMS, síťového hardwaru, připojených zařízení a kabeláže v definovaných intervalech. Je nezbytné vést přesný soupis všech serverů a zařízení včetně jejich umístění.

Správa softwaru

Zásady používání softwaru třetích stran

Jelikož se systém instaluje do standardního prostředí systému Windows, může být lákavé využívat toto prostředí pro softwarové aplikace, které nesouvisejí se správou videa. Instalace dalších aplikací třetích stran otevírá možnost proniknutí škodlivého softwaru do prostředí, což může vést k výpadkům systému nebo poskytnout útočníkovi zadní vrátka pro vstup do sítě organizace.

Doporučené zásady a postupy
Na hostitelském hardwaru nespouštějte nic jiného než software serveru a důvěryhodné integrace třetích stran. Pokud je třeba fyzický hardware využít k jiným účelům, doporučuje se použít více instancí virtuálních serverů a spustit software serveru na jednom virtuálním počítači a software třetích stran nesouvisející se systémem VMS na jiném virtuálním počítači. Informace o provozování systému ve virtuálním prostředí naleznete *zde*.

Doporučujeme nasadit antivirový software na všechny servery a počítače, které se připojují k serveru . V případě nasazení mobilních zařízení je třeba zajistit, aby byla tato zařízení vybavena nejnovějšími operačními systémy a opravami (nikoli však přímo antivirem). Při skenování pomocí antivirového softwaru neprovádějte skenování adresářů a podadresářů, které obsahují databáze záznamů. Vyhledávání virů v těchto adresářích může ovlivnit výkon systému.

Správa účtů

Obecné zásady týkající se účtu

Z důvodu pohodlí jsou někdy běžným uživatelům udělována práva na úrovni správce. V mnoha organizacích není jasně vymezeno, kdo je zodpovědný za kontrolu oprávnění účtů a monitorování přístupu zaměstnanců k systémům.

Doporučené zásady a postupy
Doporučujeme, aby se organizace při definování systémových účtů řídily zásadou nejmenších nutných oprávnění. To znamená, že přístupová práva uživatelů jsou omezena pouze na prostředky potřebné k provádění jejich konkrétních pracovních úloh. Doporučuje se také pravidelně kontrolovat oprávnění účtů uživatelů systému, aby se předešlo nežádoucímu postupnému rozšiřování oprávnění.

Zásady účtů správce systému

Častou chybou při nasazování systému v prostředí Windows je, že je pro hostitele systému Windows definován jediný účet správce. Postupem času může dojít ke sdílení hesla v rámci organizace a ke vzniku rizika, že neoprávněné osoby získají oprávnění správce prostředí systému Windows. To může snadno vést k tomu, že na daný server budou nainstalovány nežádoucí uživatelské aplikace nebo malware.

Doporučené zásady a postupy
Počítač se systémem Windows hostující server by měl mít alespoň jeden účet s oprávněním správce a jeden účet s oprávněním

uživatele. Žádný z těchto účtů by neměl být stejný jako výchozí účet správce systému Windows. Výchozí účet správce by měl být deaktivován po vytvoření účtů s oprávněním správce a účtu s oprávněním uživatele. Po nasazení by heslo účtu správce měli znát a používat pouze **správci sítě**. Účet s oprávněním uživatele by měl používat **správce video systému**, pokud se bude potřebovat přihlásit k serveru . Je třeba poznamenat, že i pokud bude obě výše uvedené role vykonávat stejná osoba, doporučuje se pro účely auditu používat oddělené účty správce sítě a účty správce video systému. Pro potřeby dalších dříve definovaných rolí by měly být pro každého jednotlivého **uživatele**, který se bude přihlašovat k systému, vytvořeny další neprivilegované uživatelské účty.

Pokud je hostitel provozující systém umístěn v doménovém prostředí služby Active Directory systému Windows, lze v rámci domény vytvořit účty správce a uživatelské účty nebo lze k ověřování hostitele systému použít existující doménový účet zaměstnance. To může zjednodušit správu účtů, protože není třeba vytvářet a spravovat další účty. To také otevírá možnost použití správy zásad skupiny k vynucování složitosti hesel, nasazování certifikátů a dalších funkcí zabezpečení dostupných v doménových prostředích.

Zásady pro uživatelské účty systému

V systému jsou uživatelským účtům přiřazeny konkrétní role, které následně určují konkrétní oprávnění každého uživatele v systému, například k jakým pohledům a videím má uživatel přístup. Pokud jeden uživatelský účet sdílí více osob, zvyšuje se riziko sdílení hesla s dalšími osobami v organizaci. Sdílení účtů také prakticky znemožňuje auditování toho, kdo a kdy přistupoval k jaké kameře/videu.

Doporučené zásady a postupy

Pokud je to možné, použijte službu Microsoft Active Directory pro snadnou správu uživatelů a skupin. Před nastavením systému se rovněž doporučuje ověřit, zda byly pro všechny uživatelské role definovány příslušné bezpečnostní skupiny.

Služba Active Directory navíc zajišťuje:

- Zásady používání hesel, které vyžadují, aby uživatelé pravidelně měnili svá hesla.
- Ochranu před útoky hrubou silou, která zajistí zablokování účtu Windows AD po několika neúspěšných pokusech o ověření v souladu s zásadami používání hesel organizace.
- Oprávnění založená na rolích, což umožňuje uplatňovat řízení přístupu v celé doméně.

Pokud je nutné používat místní účty systému Windows, doporučujeme aby byl pro každého uživatele systému vytvořen jedinečný účet a aby měl přístup pouze k těm entitám v systému, které jsou nezbytné pro plnění jeho povinností. Využití skupin pro uživatele může zjednodušit přidělování oprávnění, pokud existuje více uživatelů se stejnými oprávněními.

Zásady účtů zařízení

Účty v zařízeních Axis jsou primárně účty počítačů/klientů. **Uživatelům** by nikdy neměl být umožněn přímý přístup k zařízení. Jediným klientem, který by měl k zařízení přistupovat za běžného provozu, je server . Běžnou strategií je, že všechna zařízení používají stejné heslo. To přináší další rizika, ale současně může i zjednodušit správu hesel, takže je třeba vyhodnotit míru vlastní tolerance k riziku. Systém podporuje přiřazení jedinečných hesel ke každému zařízení prostřednictvím rozhraní pro správu.

Častou chybou je, že zařízení jsou do systému přidávána s jedním účtem, který sdílí více rolí. V určitém okamžiku, kdy **technik video systému** potřebuje použít prohlížeč, aby něco upravil, dojde k prozrazení hesla hlavního účtu (root) zařízení. Během několika měsíců bude většina lidí v organizaci znát heslo ke všem zařízením a bude mít oprávnění správce systému.

Doporučené zásady a postupy
Zařízení by mělo používat alespoň dva účty správce: jedinečný účet vytvořený pro správce zařízení a výchozí účet root pro přidávání zařízení na server . Dočasný přístup, například když **technik video systému** přistupuje k zařízení pomocí webového prohlížeče, by měl být řešen pomocí dočasných účtů.

Nástroj AXIS Device Manager by měl být používán jako primární nástroj pro správu účtů a hesel zařízení. Verze nástroje AXIS Device Manager je integrována přímo do systému a je k dispozici na kartě Management (Správa). Heslo root zařízení by měl používat pouze nástroj AXIS Device Manager a systém a měli by ho znát pouze ti, kteří používají nástroj AXIS Device Manager nebo systém jako nástroj pro správu zařízení.

Pomocí systému zřiďte dočasný účet, pokud někdo v roli technika potřebuje použít webový prohlížeč pro přístup k zařízení(m) za účelem řešení problémů nebo údržby. Vyberte zařízení a vytvořte nový účet, pokud možno s oprávněními obsluhy, který může technik využít. Po dokončení úlohy dočasný účet odstraňte.

Zásady zabezpečení systému

Údržba systému

– zásady instalace oprav hostitele Windows

Server a klienti běží v prostředí Windows. Je důležité tyto systémy pravidelně aktualizovat, aby bylo zajištěno, že systémy hostující software nemají neošetřené zranitelnosti, které by bylo možné zneužít k získání neoprávněného přístupu do systému pro správu videa.

Doporučené zásady a postupy
U všech systémů , ať už jsou provozovány prostřednictvím Axis NVR nebo na vlastním hardwaru, se doporučuje vypnout automatické aktualizace. Aktualizace systému Windows v minulosti způsobovaly nestabilitu základního operačního systému Windows, proto se doporučuje, aby se dostupné aktualizace testovaly na vybraných počítačích a zajistila se tak stabilita systému před jejich rozšířením do všech hostitelských systémů se softwarem . Je však třeba najít rovnováhu mezi bezpečností a stabilitou, protože příliš dlouhé ponechání systému Windows bez oprav může vyvolat riziko pro celé prostředí. Na základě úrovně vystavení systému zákazníka vnějším hrozbám by měl být v zásadách instalace oprav stanoven časový rámec pro zajištění toho, aby byly v systémech nainstalovány nejnovější aktualizace.

Zásady aktualizace softwaru

Ve většině případů vám používání nejnovější softwarové verze systému zajistí, že budete využívat bezpečnostní opravy pro všechny nově objevené zranitelnosti. Ponecháte-li systém delší dobu bez oprav, zvýší se riziko, že případný útočník zneužije zranitelnosti a ohrozí systém.

Doporučené zásady a postupy
Pro zajištění aktuálnosti systému je důležité definovat zásady instalace oprav s pravidelným vyhodnocováním nasazených verzí softwaru. Zásady instalace oprav by také měly určit, kdo je zodpovědný za řízení prací spojených s aktualizací serverového i klientského softwaru. Nejnovější vydání softwaru naleznete na *www.axis.com*. Software vyžaduje nejnovější knihovny .NET, takže je třeba dbát na sladění zásad instalace oprav systému Windows se zásadami softwaru .

Zásady aktualizace firmwaru zařízení

Provozování zařízení s aktuálními verzemi firmwaru zmírňuje většinu běžných rizik, protože nejnovější verze firmwaru obsahují opravy známých zranitelností, které se útočníci mohou pokusit zneužít. Společnost Axis poskytuje dlouhodobou podporu (LTS) pro firmware zařízení, která zahrnuje bezpečnostní opravy a opravy chyb, přičemž přidávání funkcí je omezeno, aby byla zajištěna dlouhodobá stabilita platformy. Další informace o strategii společnosti Axis v oblasti vývoje firmwaru naleznete v dokumentu whitepaper *Axis firmware management*.

Doporučené zásady a postupy
U hardwarových zařízení musí zásady stanovovat, že veškerý firmware musí být pravidelně aktualizován. Procesy mohou využívat vestavěnou funkci aktualizace firmwaru v systému nebo nástroji AXIS Device Manager Extend, za účelem zjištění toho, zda jsou k dispozici nové verze firmwaru pro zařízení Axis. Je vhodné definovat plánovaný čas, obvykle mimo pracovní dobu, kdy budou instalovány aktualizace firmwaru pro všechny kamery. / AXIS Device Manager Extend může také ověřit, zda byly aktualizace firmwaru přijaty. Pokud má systém specifické integrace, které by mohly být aktualizací ovlivněny, zvažte standardizaci na řadu firmwaru LTS.

Zabezpečení sítě

Zásady vzdáleného přístupu

U zařízení a služeb připojených k internetu se zvyšuje riziko toho, že dojde k prozkoumávání nebo zneužití známých zranitelných míst ze strany vnějších útočníků. Kamery vystavené internetu, například v malých organizacích vyžadujících vzdálený přístup k videu, se stávají snadnou obětí, pokud jsou použita slabá hesla nebo je objevena nová kritická zranitelnost. Vzdálený přístup k prostředí systému Windows je třeba přísně omezovat nebo mu pokud možno zamezit. Ačkoli prostředí systému Windows může mít připojení k internetu, neboť to usnadňuje aktualizaci systémů, používání služeb vzdáleného přístupu k ploše, jako jsou Windows Remote Desktop, TeamViewer a AnyDesk, představuje cesty k získání přístupu k systému, pokud nejsou správně spravovány.

Doporučené zásady a postupy
Nikdy nevystavujte IP adresu / port kamery způsobem, který by ji zpřístupnil přímo z internetu. Pokud je vyžadován vzdálený přístup k videu, použijte zabezpečený vzdálený přístup Axis. používá cloudový server pro vzdálený přístup, který zprostředkovává šifrovaný vzdálený přístup k systému prostřednictvím klienta nebo mobilní aplikace AXIS Camera Station. Kromě toho, že je server pro vzdálený přístup zodpovědný za správu připojení pro vzdálené a mobilní uživatele, hraje důležitou roli při ochraně integrity při používání vzdálenými uživateli. Další informace o zabezpečeném vzdáleném přístupu Axis můžete najít *zde*. Společnost Axis dodává

oficiálně označené mobilní aplikace pro systémy Android i Apple iOS. Mobilní aplikace AXIS Camera Station musí být stažena pouze z oficiálních zdrojů, tedy z obchodu Google Play a Apple App Store.

Pokud jde o vzdálený přístup k ploše v prostředí systému Windows, nedoporučuje se poskytovat tento typ přístupu k systému, na kterém běží aplikace . Pokud je to však nutné, je třeba věnovat mimořádnou pozornost tomu, aby zvolená aplikace pro vzdálený přístup k ploše byla zabezpečená a přístup byl poskytnut pouze těm osobám, které to vyžadují. Doporučuje se zavést další úrovně řídicích mechanismů, jako je vícefaktorová autentizace (MFA). Důrazně se doporučuje zaznamenávat a následně auditovat pokusy o vzdálené připojení, aby bylo možné sledovat, kdo a v jakém čase přistupuje k prostředí systému Windows vzdáleně.

Zásady vystavení místní síti

Snížení vystavení místní síti může pomoci zmírnit mnoho běžných hrozeb tím, že zmenší povrch útoku. Existuje mnoho způsobů, jak omezit vystavení síti, včetně fyzické segmentace sítě (oddělený síťový hardware a kabely), logické segmentace sítě prostřednictvím virtuálních sítí LAN (VLAN) a filtrování IP adres. Kamery Axis podporují filtrování IP adres (IP tabulky), takže zařízení odpovídá pouze na požadavky na připojení z IP adres, které byly výslovně povoleny.

Doporučené zásady a postupy
Systémy NVR AXIS Camera Station S22 jsou hardwarové servery s duálními síťovými porty. Jeden z portů vytváří segmentovanou síť pro kamery a druhý se připojuje k primární síti (doméně) pro obsluhu video klientů. Server funguje jako most a brána firewall pro síť kamer a brání klientům v přímém přístupu ke kamerám. Tím se snižuje pravděpodobnost výskytu hrozeb ze strany útočníků v primární síti.

Pokud jsou server a kamery umístěny v primární síti, doporučujeme nakonfigurovat filtr IP kamer a omezit přístup pouze na servery hostující systém , nástroj AXIS Device Manager a další klienty pro správu.

Zásady síťového šifrování

Síťový provoz přenášený přes nezabezpečené sítě je třeba vždy šifrovat. Internet je klasifikován jako nezabezpečená síť. Místní síť může být rovněž klasifikována jako nezabezpečená, a proto by měl být síťový provoz rovněž šifrován. Zásady, které je třeba uplatnit na přenosy videa v síti, závisí na tom, jak je video klasifikováno, a na míře rizika toho, že k video systému mohou získat síťový přístup útočníci. Doporučuje se předpokládat, že síť již byla narušena. Větší organizace obvykle uplatňují zásady, které definují klasifikaci sítě.

Doporučené zásady a postupy

Komunikace mezi video klientem a serverem by měla používat šifrování. Komunikace mezi serverem a kamerami by měla používat šifrování v závislosti na infrastruktuře. Kamery Axis jsou ve výchozím nastavení vybaveny certifikátem s vlastním podpisem a aktivovaným protokolem HTTPS. Pokud existuje riziko síťového spoofingu, například když se počítač útočníka pokouší vydávat za kameru, je vhodné použít infrastrukturu soukromých klíčů (PKI) s certifikáty podepsanými certifikační autoritou. Systém disponuje vestavěnou místní certifikační autoritou (CA), která dokáže nákladově efektivně spravovat podepisování a distribuci serverových certifikátů pro zařízení Axis.

Verze TLS

Doporučujeme vypnout TLS verze 1.1 a 1.0. Instalační program systému AXIS Camera Station nabízí pomoc při instalaci nebo aktualizaci.

Šifry HTTPS

podporuje a používá sady šifer TLS k zabezpečenému šifrování připojení HTTPS. Konkrétní sada šifer závisí na klientovi, který se připojuje k systému nebo na kontaktované službě a systém ji vyjednává na základě protokolu TLS. Doporučujeme nakonfigurovat systém Windows tak, aby nepoužíval sady šifer TLS 1.2 uvedené v dokumentu *RFC 7540*. Možnost deaktivace sady šifer závisí na zařízeních a kamerách, které se používají společně se systémem . Pokud zařízení nebo kamera vyžaduje určitou sadu šifer, nemusí být možné slabou sadu šifer zakázat.

Správa dat

Klasifikace videa

Živé a zaznamenané video je třeba klasifikovat. Video může být klasifikováno jako veřejné, soukromé, s omezeným přístupem nebo v jiných kategoriích definovaných zásadami organizace. V mnoha případech je video regulováno zákony a regionálními předpisy, stejně jako interními zásadami IT, takže je odpovědností vlastníka systému znát zákony a předpisy, které se vztahují na jeho video data.

Zásady zabezpečení systému

Doporučené zásady a postupy
Klasifikujte živé video, zaznamenané video a zvuk v souladu s organizačními zásadami klasifikace dat. Přístupová práva uživatelů a posílení zabezpečení systému konfigurujte v závislosti na citlivosti video a audio dat. Pokud není zvuk vyžadován, lze jej vypnout na úrovni zařízení.

Další prvky zabezpečení

V závislosti na úrovni vyspělosti a toleranci rizik vaší organizace doporučujeme zavést několik dalších bezpečnostních mechanismů ze standardu CIS Controls v8, které pomohou snížit rizika kybernetické bezpečnosti při každodenním provozu.

Další prvky CIS:

Prvek 8: Správa protokolu auditu
Shromažďujte, kontrolujte a uchovávejte protokoly auditu událostí, které by mohly pomoci odhalit útok, porozumět mu nebo se z něj zotavit.

Prvek 14: Implementujte program zvyšování povědomí o bezpečnosti a školení
Pochopte dovednosti a chování svých zaměstnanců. Vyškolte zaměstnance v rozpoznávání různých forem útoků.

Prvek 17: Reakce na incidenty a jejich řízení
Využívejte písemné plány reakce na incidenty s jasně definovanými fázemi řešení/řízení incidentů a rolemi pracovníků, jakož i způsoby hlášení bezpečnostních incidentů příslušným orgánům a třetím stranám.

Průvodce posílením zabezpečení systému
AXIS Camera Station 5

Ver. M3.2
Datum: 2024
Katalogové č. T10179095