UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

DIPLOMOVÁ PRÁCE

2024 Dmytro Kopytin

Univerzita Pardubice

Fakulta Ekonomicko-správní

Implementace nové verze PSI DSS v maloobchodní síti

Diplomová práce

2024

Dmytro Kopytin

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Dmytro Kopytin**
Osobní číslo:	**E23806**
Studijní program:	**N0688A140007 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Implementace nové verze PSI DSS v maloobchodní síti**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je navrhnout a ověřit implementaci Payment Card Industry Data Security Standard v maloobchodní síti s cílem zvýšit bezpečnostní opatření a ochranu údajů platebních karet se zaměřením na optimalizaci procesů a splnění bezpečnostních standardů.

Osnova

- Úvod do problematiky bezpečnosti platebních karet v maloobchodě.
- Přehled Payment Card Industry Data Security Standard (PCI DSS).
- Analýza stávajících bezpečnostních opatření v maloobchodní síti.
- Optimalizace procesů pro splnění požadavků PCI DSS.
- Implementace nové verze PCI DSS v maloobchodní síti.

Rozsah pracovní zprávy: **cca 50 stran**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

COOPER, Art, Jeff HALL, David MUNDHENK a Ben ROTHKE. He Definitive Guide to PCI DSS Version 4. Berlin: Springer, 2023. ISBN 9781484292877.
GOLDOVSKÝ, Igor. Zabezpečení online plateb. Petrohrad: Piter, 2001. ISBN 5-318-00562-4.
WRIGHT, Steve. PCI DSS: A Practical Guide to implementing and maintaining compliance. Third Edition. IT Governance Publishing, 2011. ISBN 9781849281881.

Vedoucí diplomové práce: **RNDr. Ing. Oldřich Horák, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání diplomové práce: **1. září 2024**
Termín odevzdání diplomové práce: **30. dubna 2025**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

prof. Ing. Jitka Komárková, Ph.D. v.r.
garant studijního programu

V Pardubicích dne 1. září 2024

Prohlašuji**:**

Práci s názvem Implementace nové verze PSI DSS v maloobchodní síti jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně nebo doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30.04.2025 Dmytro Kopytin v.r.

Poděkování

Chtěl bych poděkovat vedoucímu mé diplomové práce panu RNDr. Ing. Oldřichu Horákovi, Ph.D., za poskytnuté cenné rady, odborné vedení, vstřícnost a trpělivost, které mi pomohly vypracování mé diplomové práce. A chtěl bych poděkovat mé rodině a kamarádům za podporu a trpělivost během mého studia na univerzitě.

ANOTACE

Diplomová práce se zabývá návrhem a implementací standardu Payment Card Industry Data Security Standard (PCI DSS) v prostředí maloobchodní sítě s cílem zvýšit úroveň bezpečnostních opatření a ochrany údajů platebních karet. Hlavním cílem je optimalizace procesů, která povede k efektivnímu splnění požadavků PCI DSS a posílení bezpečnosti citlivých platebních dat. Práce poskytuje úvod do problematiky bezpečnosti platebních karet v maloobchodě, detailní přehled standardu PCI DSS, analýzu aktuálních bezpečnostních opatření v dané síti a popis procesu optimalizace. Závěrečná část se věnuje praktické implementaci nové verze PCI DSS a zhodnocení dosažených výsledků v kontextu zvýšené ochrany a efektivity procesů.

KLÍČOVÁ SLOVA

PCI DSS, bezpečnost platebních karet, ochrana údajů, maloobchod, optimalizace procesů.

TITLE

Implementation of the new version of PCI DSS in a retail network

ANNOTATION

The thesis focuses on the design and implementation of the Payment Card Industry Data Security Standard (PCI DSS) within a retail network environment, aiming to enhance security measures and protect payment card data. The primary goal is to optimize processes, leading to effective compliance with PCI DSS requirements and strengthening the security of sensitive payment information. The work provides an introduction to the issue of payment card security in retail, a detailed overview of the PCI DSS standard, an analysis of current security measures in the network, and a description of the optimization process. The final part addresses the practical implementation of the new version of PCI DSS and evaluates the results achieved in terms of enhanced protection and process efficiency.

KEYWORDS

PCI DSS, payment card security, data protection, retail, process optimization.

OBSAH

SEZNAM OBRÁZKŮ A TABULEK

SEZNAM ZKRATEK

PCI DSS	Payment Card Industry Data Security Standard
POS	Point of sale
RAT	Remote Access Trojans
ISMS	Information Security Management System
IDS	Intrusion Detection System
IPS	Intrusion Prevention Systém
PAN	Primary Account Number
SLA	Service Level Agreements
RTO	Recovery Time Objective
RPO	Recovery Point Objective
CDE	Cardholder Data Environment
SIEM	Security Information and Event Management
GDPR	General Data Protection Regulation

ÚVOD

V posledních letech se zabezpečení platebních transakcí stalo jedním z nejdůležitějších aspektů v oblasti maloobchodu, a to především kvůli rostoucímu množství citlivých dat, která musí být chráněna před možnými útoky. S digitalizací plateb a širším používáním karet, jak fyzických, tak virtuálních, roste i riziko úniků informací a kybernetických útoků, které mohou vést k vážným finančním a reputačním následkům pro maloobchodníky. Aby byl minimalizován dopad těchto hrozeb, vznikl Payment Card Industry Data Security Standard (PCI DSS) – globální bezpečnostní standard, který definuje opatření nutná k ochraně údajů držitelů platebních karet a poskytuje směrnice pro zajištění bezpečnosti v celém transakčním procesu.

Standard PCI DSS stanovuje požadavky na zabezpečení údajů o platebních kartách, které zahrnují například šifrování dat, omezení přístupu k citlivým informacím a pravidelné testování a monitorování bezpečnostních systémů. Tyto požadavky jsou pravidelně aktualizovány, aby odpovídaly současným technologickým výzvám a hrozbám. Poslední verze PCI DSS zavádí nové postupy, které mají nejen zajistit vyšší úroveň ochrany dat, ale také podporovat efektivitu maloobchodních provozů a jejich schopnost reagovat na nové bezpečnostní požadavky a rizika.

Tato diplomová práce tak poskytuje komplexní pohled na problematiku zabezpečení platebních údajů a optimalizaci bezpečnostních opatření v maloobchodním prostředí podle nejnovějších standardů. Pro účely praktické části analýzy byla oslovena a spolupracovala společnost, která reprezentuje cílovou skupinu této práce – konkrétní maloobchodní síť s aktivním využíváním platebních karet. Díky této spolupráci bylo možné ověřit teoretické poznatky v praxi, identifikovat reálné výzvy při implementaci standardu PCI DSS a navrhnout doporučení přizpůsobená specifickému provoznímu kontextu dané firmy.

Práce rovněž obsahuje podrobný přehled jednotlivých požadavků PCI DSS a poskytuje krok za krokem návod na jejich zavedení v prostředí maloobchodu. Součástí implementace je i školení zaměstnanců a zavedení nástrojů pro průběžné monitorování a testování bezpečnostních opatření. V závěrečné části práce je provedeno hodnocení efektivity navržených opatření a jejich vlivu na celkovou úroveň bezpečnosti a efektivitu provozů v dané maloobchodní síti, přičemž jsou zohledněny reálné podmínky a omezení vyplývající z každodenního provozu. Tato diplomová práce tak poskytuje komplexní pohled na problematiku zabezpečení platebních údajů a optimalizaci bezpečnostních opatření v maloobchodním prostředí podle nejnovějších standardů.

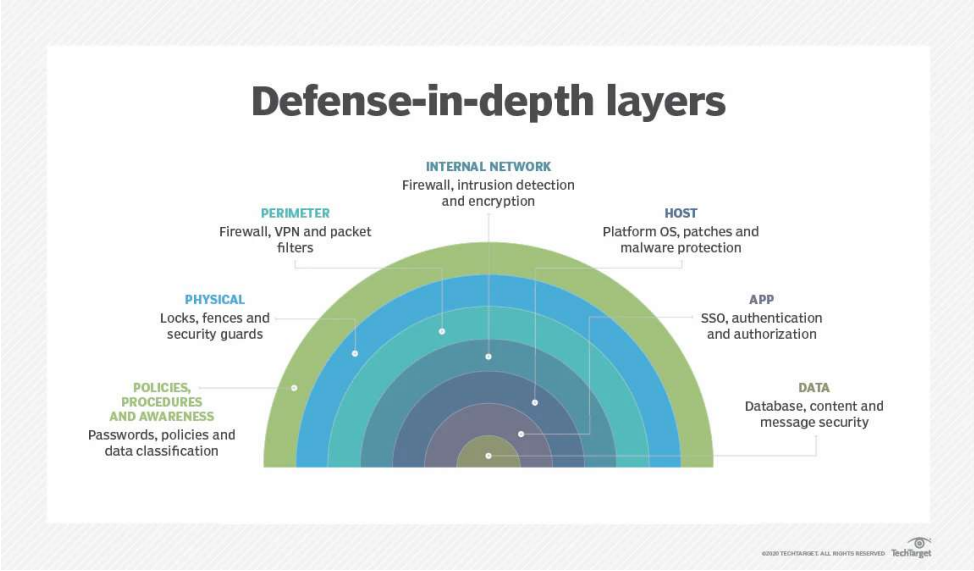
1. ÚVOD DO PROBLEMATIKY BEZPEČNOSTI PLATEBNÍCH KARET V MALOOBCHODĚ

1.1. Význam bezpečnosti platebních karet

V moderní ekonomice založené na datech, digitalizovaných procesech a neustále rostoucím propojení fyzického a digitálního prostředí se platební karty staly neoddělitelnou součástí každodenního života jak spotřebitelů, tak obchodních subjektů. Již dávno nepředstavují pouze alternativu k hotovosti – staly se primárním nástrojem pro placení v kamenných obchodech, online prostředí i v rámci mobilních aplikací. Zákazníci je používají automaticky a s očekáváním, že celý proces bude nejen rychlý a pohodlný, ale především bezpečný. Z pohledu obchodníků pak platební karty představují zásadní prvek provozní efektivity, kontroly nad peněžními toky a optimalizace zákaznické zkušenosti. Současně však tento platební mechanismus vystupuje jako velmi citlivý bod v celém hodnotovém řetězci interakce se zákazníkem. Každá jednotlivá transakce, ať už realizovaná fyzicky přes platební terminál nebo elektronicky přes e-shop, zahrnuje zpracování osobních a finančních údajů – typicky čísla karty, data platnosti, jména držitele nebo bezpečnostního kódu CVV [1]. Tyto informace patří mezi nejcitlivější typy dat vůbec, protože jejich zneužití může vést k přímým finančním ztrátám, podvodům a dalším formám kriminality. Z pohledu kybernetické bezpečnosti jsou tedy karetní údaje vysoce exponovaným cílem, a to jak pro automatizované útoky, tak pro sofistikované aktivity organizovaných skupin.

Jejich ochrana přitom není pouze technickým nebo provozním požadavkem – představuje základní předpoklad pro fungování důvěry mezi zákazníkem a obchodníkem. Spotřebitelé, kteří vnímají obchodníka jako bezpečného a transparentního partnera, jsou mnohem ochotnější provádět opakované transakce, sdílet osobní údaje nebo využívat moderní platební technologie. Naopak v případě selhání bezpečnosti často dochází k okamžitému narušení důvěry, odlivu klientely a poškození značky [2]. Ochrana karetních údajů tak přímo ovlivňuje nejen zákaznickou loajalitu, ale i dlouhodobou reputaci společnosti. Zároveň je třeba mít na paměti, že nedostatečné zabezpečení může mít i závažné právní a regulační dopady. Podniky, které zpracovávají údaje o platebních kartách, podléhají celé řadě předpisů – od mezinárodních standardů, jako je PCI DSS, až po evropské a národní legislativní rámce včetně GDPR. Nedodržení těchto požadavků může vést k pokutám, soudním sporům nebo i ztrátě oprávnění ke zpracování plateb. Bezpečnost tedy není volitelný doplněk, ale nezbytný pilíř stabilního a legálně udržitelného obchodního modelu, jehož význam bude v následujících letech dále narůstat [3; 1]. Zabezpečení karetních dat je klíčové zejména v prostředí maloobchodu, které se vyznačuje vysokou frekvencí transakcí, rozsáhlou sítí provozoven, velkým počtem zaměstnanců a často i komplexní technologickou infrastrukturou.

To vše vytváří prostředí, kde může dojít k různým typům zranitelností – od technických chyb v systémech přes lidské pochybení až po cílené útoky. Obchodníci dnes čelí tlakům nejen ze strany zákazníků, kteří očekávají maximální bezpečnost, ale také od regulačních orgánů a karetních asociací, které stanovují přísná pravidla pro práci s citlivými údaji. Význam bezpečnosti karetních údajů se ukazuje ve dvou hlavních rovinách – v rovině důvěry a reputace a v rovině provozního a právního rizika. Na straně jedné je důvěra zákazníků klíčovým faktorem, který rozhoduje o tom, zda se k obchodníkovi vrátí. Jakýkoli incident spojený s únikem dat má okamžitý negativní dopad na image společnosti. Spotřebitelé bývají v těchto situacích velmi citliví a často preferují konkurenci, která působí bezpečněji. Na straně druhé je zde aspekt provozního rizika – organizace, které selžou v oblasti bezpečnosti, se vystavují nejen přímým finančním ztrátám (např. refundace, pokuty), ale i dlouhodobým nákladům spojeným s obnovou reputace, právními spory či interní restrukturalizací bezpečnostních procesů. Zabezpečení karetních údajů však nelze zredukovat pouze na technologii [4]. Přestože nástroje jako šifrování, firewall, antivirová ochrana, detekční systémy nebo tokenizace představují důležité prvky technické obrany, samy o sobě nestačí. Skutečná bezpečnost je výsledkem komplexního systému, který propojuje technickou infrastrukturu s organizačními opatřeními, definovanými procesy a lidským faktorem. To zahrnuje mimo jiné důkladné školení zaměstnanců, jasně nastavené odpovědnosti a postupy při zjištění incidentu, pravidelné audity, simulace krizových scénářů a systematické budování bezpečnostního povědomí napříč celou firmou.



Obrázek 1 Bezpečnostní vrstvy při ochraně karetních dat (Defense in Depth)

Zdroj [4]

V prostředí maloobchodu, kde hrají klíčovou roli distribuované systémy, outsourcing, sezónní zaměstnanci a různorodé provozní podmínky, je o to důležitější budovat tzv. bezpečnostní kulturu.

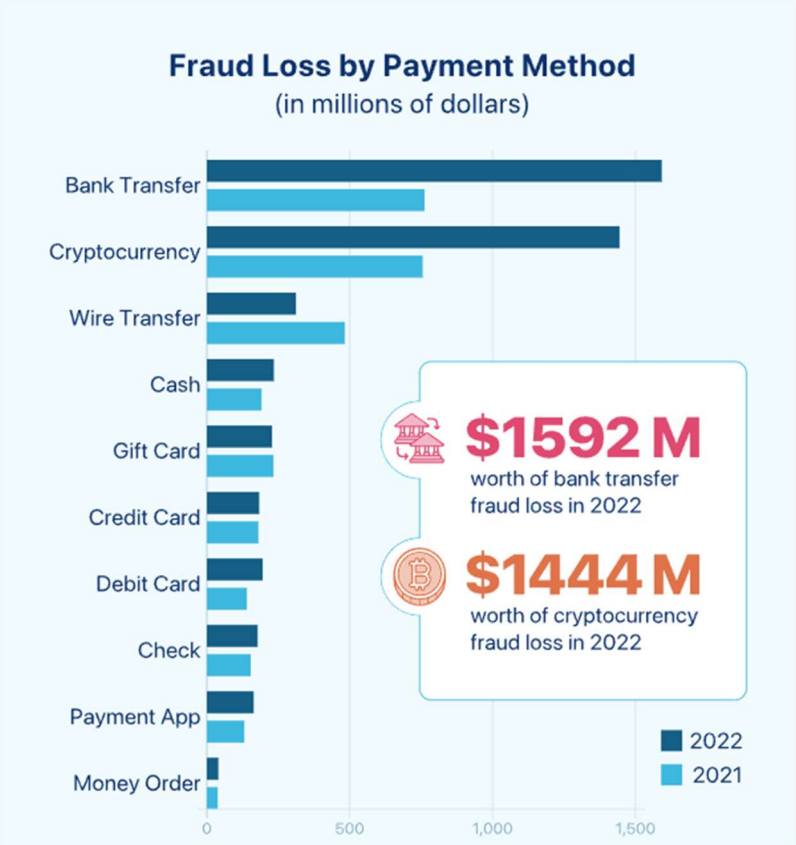
Ta znamená, že bezpečnost není vnímána jako jednorázový projekt nebo zodpovědnost IT oddělení, ale jako každodenní a společný úkol celé organizace. Jen tak lze minimalizovat riziko lidské chyby, včas rozpoznat hrozbu a efektivně reagovat na incidenty. Pokud tato kultura chybí, často selhávají i jinak dobře navržené bezpečnostní technologie – například kvůli nepozornosti zaměstnance, opomenutí při aktualizaci systému, nebo nedostatečné reakci na podezřelé chování.

S rostoucí digitalizací maloobchodu (např. samoobslužné pokladny, mobilní platby, online objednávky s osobním odběrem, zákaznické aplikace) se zároveň rozšiřuje počet potenciálních vstupních bodů pro útok. Každý nový kanál přináší nové riziko [4]. Obchodníci tak musí neustále aktualizovat svá bezpečnostní opatření, sledovat nové trendy v oblasti hrozeb a přizpůsobovat se měnícím podmínkám. Zajištění bezpečnosti již tedy není statický úkol, ale nepřetržitý proces řízení rizik, který musí být začleněn do strategického řízení celé organizace.

1.2. Trendy a hrozby v oblasti kybernetické bezpečnosti

1.2.1. Současní trendy

Bezpečnost platebních karet je ovlivňována dynamickým vývojem technologií, změnami v chování spotřebitelů a neustále se vyvíjejícím prostředím kybernetických hrozeb [5]. V posledních letech lze pozorovat několik zásadních trendů, které významně ovlivňují způsob, jakým se data o platebních kartách zpracovávají, uchovávají a chrání. Tyto trendy zásadně mění charakter rizik, jimž organizace čelí, a vyžadují odpovídající úpravy bezpečnostních opatření i strategií. Jedním z nejvýznamnějších trendů je rychlý růst bezkontaktních a mobilních platebních metod. Díky širokému rozšíření NFC technologií a platforem jako Apple Pay, Google Pay či různých aplikací bank a obchodníků se mění tradiční model zpracování karetních transakcí [6]. Zákazníci si zvykli na okamžité a pohodlné platby pomocí chytrých zařízení. Tento posun však přináší nové bezpečnostní výzvy, protože citlivé údaje se přesouvají do mobilních operačních systémů a digitálních peněženek, kde se stávají cílem sofistikovanějších útoků, často kombinujících sociální inženýrství a zneužití mobilních zranitelností. Další zásadní změnou je intenzivní přesun transakcí do online prostředí, zejména v důsledku pandemie COVID-19, která akcelerovala rozvoj e-commerce [3]. Obchodníci se často ocitli v situaci, kdy museli rychle rozšiřovat nebo přestavovat své digitální platformy bez dostatečné přípravy v oblasti bezpečnosti. V důsledku toho roste počet útoků na webové platební brány, phishingových kampaní zaměřených na krádež karetních údajů a zneužití slabých autentizačních mechanismů. Útočníci rovněž využívají tzv. botnety a automatizované skripty k testování odcizených čísel karet v reálném čase.



Obrázek 2 Vývoj nejčastějších kybernetických hrozeb v oblasti platebních karet

Zdroj [7]

Výrazně se rozvíjí také techniky útoků cílené na zranitelná koncová zařízení, zejména platební terminály (POS). Malware zaměřený na POS systémy zůstává jedním z nejběžnějších nástrojů kybernetických skupin, které se snaží získat přístup k paměti terminálů, kde se dočasně uchovávají nezašifrovaná data. I přes pokrok v oblasti šifrování a tokenizace se ukazuje, že fyzické zabezpečení zařízení a kontrola přístupu v provozovnách jsou stále podceňovány, zvláště v decentralizovaných maloobchodních sítích. Neméně důležitým trendem je rostoucí tlak na dodržování regulačních a bezpečnostních standardů, včetně PCI DSS, GDPR a dalších lokálních nařízení. Organizace jsou pod neustálým dohledem, a to nejen ze strany dozorových úřadů, ale také od samotných zákazníků, kteří si stále více uvědomují hodnotu svých dat. Transparentní a efektivní komunikace o bezpečnostních opatřeních se stává součástí obchodní strategie, a firmy, které působí důvěryhodně, získávají konkurenční výhodu.

V neposlední řadě se mění i přístup útočníků, kteří čím dál častěji využívají kombinované, vícefázové útoky a tzv. laterální pohyb v síti [8]. To znamená, že počáteční vektor útoku nemusí přímo souviset s platebním systémem – útočníci často začínají průnikem přes e-mailový phishing, slabiny v interní síti nebo kompromitovaný účet zaměstnance, a teprve následně se přesunují

do segmentu, kde jsou zpracovávány karetní údaje. Tento trend potvrzuje nutnost budovat vícevrstvou obranu a celopodnikový přístup k bezpečnosti.

1.2.2. Typy kybernetickch útoků

S rostoucí digitalizací maloobchodu a nárůstem bezhotovostních plateb se rozšiřuje i spektrum útoků zaměřených na platební systémy. Útočníci využívají kombinaci technických zranitelností, lidských chyb a nedostatečně nastavených bezpečnostních procesů k tomu, aby získali přístup k citlivým údajům o platebních kartách nebo kompromitovali celou infrastrukturu obchodníka. Níže jsou uvedeny nejčastější typy kybernetických útoků, které se objevují v prostředí, kde dochází ke zpracování karetních transakcí [9] [4].

1. Útoky na POS (Point of Sale) zařízení

Útoky na platební terminály patří mezi nejrozšířenější formy útoků v maloobchodním prostředí. Zahrnují instalaci škodlivého softwaru (např. memory scrapers), který sbírá karetní údaje přímo z paměti zařízení ještě před jejich zašifrováním. Takové útoky jsou obzvláště nebezpečné, protože probíhají často bez povšimnutí a mohou být aktivní celé týdny. Příkladem je známý útok na řetězec Target (USA), kde bylo kompromitováno více než 40 milionů platebních karet.

2. Phishing a sociální inženýrství

Phishingové kampaně cílí na zákazníky i zaměstnance. Zákazníci jsou podvedeni falešnými e-maily nebo stránkami, které imitují legitimní obchodníka či banku a vylákají z nich údaje o platební kartě. Zaměstnanci obchodníků mohou být cílem tzv. spear-phishingu, kdy útočník získá přihlašovací údaje nebo administrátorský přístup do systémů, jež zpracovávají transakce. Tyto útoky jsou často vstupní branou pro sofistikovanější průniky do interní sítě.

3. Skimming a fyzická manipulace

Skimming je metoda, při níž útočník fyzicky upraví platební zařízení (např. přidá nelegální čtecí jednotku nebo kameru), aby získal údaje z magnetického proužku karty a případně i PIN kód. Tento typ útoku je častější u samoobslužných zařízení (např. čerpací stanice, automaty), kde je nižší kontrola ze strany personálu. Novější variantou je tzv. shimmer – zařízení určené pro čtení čipových karet.

4. Malware v interní síti

Po úspěšném phishingu nebo jiném vektoru se útočník často snaží proniknout hlouběji do podnikové sítě. Malware (např. keyloggery, trojské koně nebo RAT – Remote Access Trojans) může sloužit k získání přihlašovacích údajů, sběru logů nebo aktivnímu ovládání systémů.

Typickým cílem je tzv. Cardholder Data Environment (CDE), kde se nachází citlivé transakční údaje. Malware se často šíří i laterálně, tedy mezi jednotlivými systémy uvnitř sítě [10].

5. Útoky na webové platební brány (e-skimming, formjacking)

V e-commerce prostředí je častým cílem samotný platební formulář. Útočník kompromituje kód na stránce nebo infikuje JavaScript třetí strany, který následně odesílá zadávané údaje o kartě na server útočníka. Tento typ útoku je obtížně detekovatelný, protože z pohledu zákazníka vypadá vše jako běžná platba. Oběti často zjistí problém až při zneužití údajů.

6. Brute-force a credential stuffing

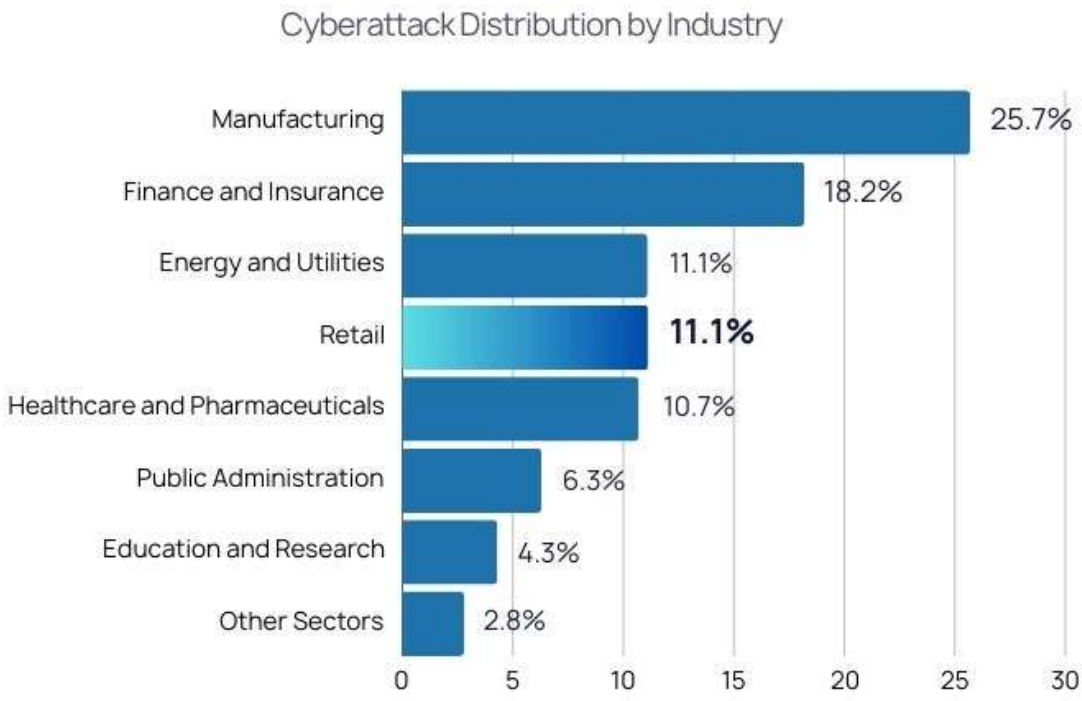
Automatizované útoky, při nichž útočníci testují obrovské množství kombinací přihlašovacích údajů (brute-force), nebo zneužívají údaje z jiných úniků (credential stuffing), jsou časté především u zákaznických účtů v e-shopech. Pokud obchodník umožňuje opakované přihlašování bez detekce podezřelé aktivity nebo nevyužívá vícefaktorovou autentizaci, může dojít ke zneužití účtu a následně i uložených platebních metod.

7. Útoky zneužívající zranitelnosti software

Zastaralé systémy, neaktualizovaný firmware na terminálech, nebo špatně nakonfigurované servery mohou být zneužity pomocí známých zranitelností (např. CVE). Útočník může získat přístup k systémům nebo obejít autentizaci. Pravidelné skenování a patch management jsou zásadní prevencí těchto typů útoků.

1.2.3. Dopady na maloobchodní sektor

Kybernetické útoky zaměřené na platební systémy mají v maloobchodním prostředí často velmi konkrétní a závažné důsledky. Maloobchodníci se denně pohybují v prostředí, kde se zpracovávají tisíce až miliony transakcí, a jakékoli narušení těchto procesů se okamžitě projeví v každodenním provozu i v celkové důvěryhodnosti firmy. Bezpečnost již není pouze otázkou technického nastavení, ale i reputační a ekonomické stability.



Obrázek 3 Řetězec dopadů kybernetického útoku v maloobchodě

Zdroj [11]

Úspěšný útok, při kterém dojde k úniku dat o platebních kartách, může pro firmu znamenat přímé finanční ztráty. Ty vznikají nejen z důvodu kompenzací zákazníkům nebo nákladů na forenzní analýzu incidentu, ale také v podobě sankcí od karetních asociací, ztráty obchodních partnerů nebo přerušení smluv s poskytovateli platebních služeb [12]. Kromě toho je nutné počítat s investicemi do nápravy, výměny technologií a obnovy důvěry. Tyto dopady jsou přímé, měřitelné a obvykle se projeví okamžitě po incidentu. Ještě závažnější však bývá dlouhodobé poškození důvěry zákazníků. V maloobchodě, kde jsou nákupy často rutinní a založené na návycích, může být narušení vnímání bezpečnosti rozhodujícím faktorem, proč se zákazník obrátí ke konkurenci. Ztráta důvěry má obvykle pomalejší, ale trvalejší dopad než samotná finanční ztráta – a návrat ke stavu před incidentem bývá náročný a nejistý. Obzvlášť u menších nebo lokálních řetězců může podobný incident vést k zásadnímu oslabení jejich pozice na trhu.

Právní stránka věci představuje další dimenzi dopadu. Obchodník má podle zákona povinnost incidenty nahlásit, spolupracovat s úřady a zároveň vysvětlit zákazníkům, co se stalo a jaká opatření byla přijata [13]. V případech, kdy se prokáže, že organizace selhala v základní prevenci nebo neplnila předepsané standardy, hrozí nejen sankce, ale také soudní žaloby ze strany poškozených osob nebo institucí. Pro firmu to znamená ztrátu času, energie i reputace, což může ovlivnit i její schopnost financování nebo získávání nových partnerů. V mnoha případech má útok

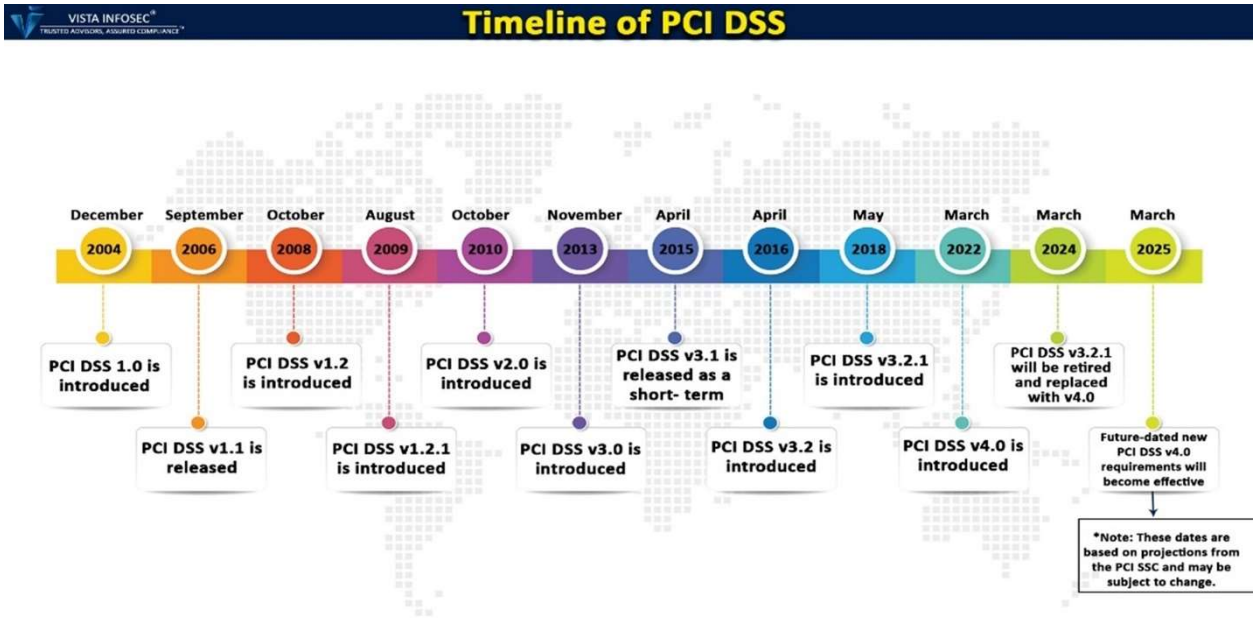
také přímý dopad na provoz firmy. Výpadky platebních systémů, odstavení poboček nebo omezení funkcionality mohou znamenat nejen ztrátu tržeb, ale také tlak na zaměstnance a nutnost improvizovaného krizového řízení. Tyto situace často odhalí i další slabiny v organizaci – například nejasné procesy, nedostatečné školení nebo chybějící plán reakce na incident.

Zásahy kybernetických útoků do maloobchodního prostředí mají zpravidla komplexní dopad – od okamžitých finančních ztrát, přes narušenou důvěru zákazníků, až po nutnost hlubších vnitrofiremních změn [11]. Právě rozsah a závažnost těchto rizik způsobují, že ochrana platebních dat se stala klíčovým prvkem moderního řízení maloobchodních firem. Aby se těmto hrozbám dalo čelit efektivně a systematicky, byly vytvořeny mezinárodní bezpečnostní standardy, které firmám poskytují jasný rámec pro prevenci i reakci.

2. PŘEHLED PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

2.1. Historie a vývoj PCI DSS

S rostoucím využíváním platebních karet v průběhu 90. let začaly karetní společnosti čelit stále častějším incidentům spojeným s únikem citlivých údajů. Vzhledem k tomu, že každá organizace měla své vlastní bezpečnostní požadavky, vznikalo roztříštěné prostředí, které bylo náročné jak na správu, tak na zajištění konzistence bezpečnostních opatření napříč odvětvím. Tento stav vedl k potřebě vytvořit jednotný a závazný rámec, který by stanovil minimální bezpečnostní standardy pro všechny subjekty, jež pracují s údaji o držitelích platebních karet [14].



Obrázek 4 Časová osa PCI DSS

Zdroj [14]

V roce 2004 proto vznikla aliance Payment Card Industry Security Standards Council (PCI SSC), kterou založily hlavní globální karetní společnosti – Visa, Mastercard, American Express, Discover a JCB. Jejím hlavním cílem bylo vytvořit společný bezpečnostní standard, který by zohledňoval jak technické, tak organizační aspekty ochrany karetních údajů v celém transakčním řetězci – od momentu zadání dat až po jejich zpracování a případné uložení. Výsledkem této snahy byl první oficiální dokument Payment Card Industry Data Security Standard (PCI DSS), jehož první verze byla zveřejněna v roce 2004. Od té doby prošel standard několika revizemi, přičemž každá nová verze reagovala na aktuální technologický vývoj a měnící se hrozby. Například verze 2.0 z roku 2010 přinesla větší důraz na řízení přístupů a šifrování dat, zatímco verze 3.0 a 3.2 rozšířily požadavky na školení zaměstnanců, testování zranitelností a řízení změn v infrastruktuře.

Standard se tak postupně vyvíjel z dokumentu s převážně technickými doporučeními do komplexního rámce, který pokrývá jak technologii, tak i lidský faktor a procesní řízení bezpečnosti.

Zatím poslední verze – PCI DSS 4.0 – byla oficiálně zveřejněna v březnu 2022 s přechodným obdobím do roku 2025. Tato verze reflektuje potřebu větší flexibility v přístupu k bezpečnosti, podporuje tzv. „zero trust“ modely a zdůrazňuje kontinuální procesy namísto jednorázového auditu [1]. Zavádí také nové koncepty, jako je customized approach (přístup založený na cílech) a důraz na cílenou analýzu rizik, která má organizacím umožnit větší prostor pro kreativní, ale stále kontrolované řešení bezpečnostních požadavků. Vývoj PCI DSS tak ukazuje, jak se kybernetická bezpečnost v oblasti platebních systémů proměňuje – od reaktivního zabezpečení konkrétních komponent až po strategický a proaktivní přístup k ochraně celé infrastruktury. Historie tohoto standardu zároveň potvrzuje, že oblast platebních dat není statická, ale vyžaduje neustálou adaptaci na nové technologie, hrozby i regulační prostředí.

2.2. Klíčové požadavky a zásady PCI DSS

2.2.1. Ochrana údajů držitelů karet

Jedním z hlavních cílů standardu PCI DSS je zajištění důsledné ochrany citlivých údajů držitelů platebních karet (tzv. cardholder data). Tato data zahrnují především číslo karty (Primary Account Number – PAN), jméno držitele, datum expirace a bezpečnostní kód (např. CVV/CVC), případně další informace z magnetického proužku nebo čipu. Únik těchto údajů může vést k jejich zneužití, podvodům a vážnému narušení důvěry mezi zákazníkem a obchodníkem. Právě proto jsou požadavky na ochranu těchto dat jedním z nejpřísněji sledovaných aspektů celého standardu.

Standard PCI DSS vyžaduje, aby údaje o kartách byly chráněny během celého životního cyklu – od okamžiku jejich zadání až po případné uložení nebo bezpečné zničení [15] [12]. Zásadním principem je, že není-li pro daný účel nezbytné uchovávat karetní data, měla by být okamžitě odstraněna nebo anonymizována. Pokud jejich uchování nezbytné je (např. kvůli reklamacím či reportingovým požadavkům), musí být implementována robustní opatření k jejich ochraně. Jedním ze základních požadavků je šifrování údajů – a to jak při přenosu (např. mezi POS terminálem a serverem), tak při jejich ukládání. Ukládání samotného bezpečnostního kódu (CVV/CVC) po autorizaci transakce je výslovně zakázáno. PAN musí být buďto silně zašifrován, nebo maskován tak, aby z něj nebylo možné odvodit plné číslo karty. Nejčastěji se používá metoda zobrazení pouze posledních čtyř číslic. Dalším opatřením je segmentace sítě a kontrola přístupu. Informace o držitelích karet by měly být dostupné pouze těm osobám a systémům, které je

skutečně potřebují k výkonu své činnosti. Přístup musí být řízen, evidován a pravidelně revidován. Kromě toho je důležitá i ochrana fyzického prostředí – například bezpečné uchovávání papírových záznamů nebo zabezpečení přístupu k serverům a zálohám. S ohledem na současné hrozby se v praxi stále více uplatňuje také tokenizace, tedy nahrazení reálných karetních údajů jednorázovými, bezvýznamovými tokeny, které nemohou být samostatně zneužity. Tímto způsobem lze minimalizovat množství citlivých dat, která se nacházejí v systému obchodníka, a tím snížit i celkové riziko. Ochrana údajů držitelů karet je základním pilířem bezpečnosti platebních systémů. Selhání v této oblasti neznamená jen riziko zneužití dat, ale i přímé finanční, právní a reputační důsledky. Proto PCI DSS stanovuje jasná a striktní pravidla, která mají za cíl snížit pravděpodobnost zneužití na minimum. Dodržování těchto pravidel není pouze otázkou souladu s normou, ale nezbytnou součástí zodpovědného přístupu k ochraně zákazníků.

2.2.2. Správa přístupových práv

Správa přístupových práv představuje jednu z klíčových oblastí ochrany citlivých údajů o držitelích platebních karet. Podle standardu PCI DSS není dostatečné citlivá data pouze šifrovat nebo tokenizovat – je stejně důležité zajistit, aby k těmto údajům měli přístup výhradně oprávněné osoby a systémy, a to přesně v rozsahu, který nezbytně odpovídá jejich pracovní roli [16] [15]. Zamezení neoprávněnému přístupu je totiž jedním z nejúčinnějších způsobů, jak minimalizovat riziko zneužití dat – a to jak zevnitř organizace, tak zvenčí.

PCI DSS vyžaduje, aby každá osoba s přístupem k citlivým informacím měla jedinečný uživatelský identifikátor (ID). Tím je zajištěna zpětná dohledatelnost aktivit v systému – pokud dojde k incidentu, lze přesně určit, kdo, kdy a jakým způsobem s daty pracoval. Používání sdílených nebo univerzálních účtů je zakázáno, protože znemožňuje sledovat individuální odpovědnost. Vedle toho musí být implementována pravidla principu nejmenších oprávnění (least privilege). Znamená to, že uživatelé mají přístup pouze k těm datům a funkcím, které nezbytně potřebují ke své práci – a nic víc. Oprávnění by se měla přidělovat podle předem definovaných rolí (role-based access control) a pravidelně revidovat, zejména při změně pozice zaměstnance, odchodu z firmy nebo přesunu mezi odděleními. Zastaralé, zbytečné nebo nadměrné přístupy představují vážné riziko, protože mohou být snadno zneužity – úmyslně i neúmyslně. Další důležitou součástí je autentizace přístupu, tedy ověření identity uživatele. PCI DSS doporučuje a ve vybraných případech i vyžaduje vícefaktorové ověření (MFA), zejména pokud se jedná o vzdálený přístup nebo administraci systémů zpracovávajících karetní údaje. Kombinace hesla a druhého faktoru – například kód zaslaný do mobilního telefonu nebo biometrické ověření – výrazně zvyšuje bezpečnost, i v případě úniku hesla [15]. Všechny pokusy o přístup – úspěšné

i neúspěšné – musí být logovány a monitorovány. Tyto záznamy slouží nejen k detekci podezřelého chování (např. opakované pokusy o přihlášení, přístupy mimo pracovní dobu), ale i k forenzní analýze v případě bezpečnostního incidentu. Logy musí být chráněny před manipulací a uchovávány po stanovenou dobu.Důraz je kladen také na procesní rámec – kdo může přístup schvalovat, jak probíhá žádost, kdy se přístupy revidují a kdo je za ně odpovědný. Pokud tyto kroky nejsou jasně nastaveny, může dojít k neřízenému rozšiřování přístupů a ztrátě kontroly nad tím, kdo má ke kterým datům přístup. Efektivní správa přístupových práv je zásadní nejen z hlediska bezpečnosti, ale také kvůli plnění požadavků auditu PCI DSS. Nedostatečná kontrola přístupů patří mezi nejčastější důvody neúspěšné certifikace nebo následného postihu po incidentu. Zavedení přehledné, pravidelně aktualizované a technicky podložené správy oprávnění proto patří mezi základní kameny každého bezpečnostního programu pracujícího s platebními kartami.

2.3. Důsledky nedodržení standardů

Nedodržování požadavků stanovených ve standardu PCI DSS může mít pro organizace závažné a mnohdy i dlouhodobé následky. Ačkoli samotný standard není zákonem v pravém slova smyslu, jedná se o povinný rámec daný smluvními podmínkami mezi obchodníkem, poskytovatelem platebních služeb a karetními asociacemi. V praxi to znamená, že každá organizace, která zpracovává, uchovává nebo přenáší údaje o platebních kartách, je povinna tento rámec dodržovat – a jeho porušení může mít jak finanční, tak právní a provozní důsledky. Mezi nejčastější formy postihu patří vysoké pokuty ze strany karetních společností, které mohou v závislosti na rozsahu pochybení dosahovat statisícových až milionových částek [17]. Pokuty nejsou jednorázové – v případě, že organizace zůstává mimo shodu (non-compliant) po delší dobu, mohou být účtovány opakovaně, a to až do nápravy stavu. Kromě toho může být obchodník povinen hradit náklady na nahrazení karet dotčených zákazníků, kompenzovat vzniklé škody a uhradit náklady na forenzní vyšetřování incidentu. Z hlediska smluvních vztahů je jedním z nejzásadnějších rizik ztráta oprávnění přijímat platební karty, případně omezení přístupu ke zpracovatelským službám. Takové opatření může mít pro maloobchodní společnost fatální dopady, protože bez možnosti přijímat karty ztrácí konkurenční výhodu, snižuje obrat a přichází o důvěru zákazníků. Některé společnosti navíc v případě incidentu musí uzavřít tzv. monitoring agreement – tedy povinný dohled s pravidelnými audity a reportováním vůči karetním asociacím, což dále zatěžuje vnitřní kapacity firmy. Reputace je další oblast, která bývá výrazně narušena. Jakmile dojde ke zveřejnění incidentu – a to se dle GDPR nebo zákonných rámců obvykle musí stát – ztrácejí zákazníci důvěru ve schopnost organizace chránit jejich údaje. V médiích i na sociálních sítích se bezpečnostní selhání rychle šíří a má potenciál způsobit vážné poškození značky. Zákazníci pak častěji volí

konkurenci a návrat k původní úrovni důvěry může trvat měsíce až roky [18]. Nedodržování PCI DSS může mít i právní důsledky. V případě úniku dat jsou firmy povinny incident nahlásit úřadům podle GDPR a dalších národních předpisů [17]. Pokud se prokáže, že organizace zanedbala přiměřená bezpečnostní opatření (což PCI DSS definuje velmi konkrétně), může být uložena regulační pokuta. Navíc hrozí soudní spory ze strany poškozených zákazníků, pojišťoven nebo obchodních partnerů, kteří kvůli incidentu utrpěli škodu. Nelze opomíjet ani vnitřní dopady, které jsou méně viditelné, ale neméně důležité. Organizace, která čelí bezpečnostnímu incidentu a neprošla auditem PCI DSS, musí obvykle provést okamžitou reorganizaci procesů, aktualizaci dokumentace, přechod na nové technologie a zavést rozsáhlá školení zaměstnanců. Tyto kroky představují vysoké finanční i personální náklady, které přicházejí často v krizové situaci, kdy je firma pod tlakem a řeší následky incidentu.

Tabulka 1 Důsledky Nedodržení PCI DSS

Typ důsledku	Popis dopadů
Finanční	Pokuty od karetních asociací, náklady na výměnu karet, forenzní šetření, kompenzace zákazníkům.
Právní	Hlášení úniku podle GDPR, regulační pokuty, soudní žaloby od zákazníků nebo partnerů.
Reputační	Ztráta důvěry zákazníků, poškození značky, negativní mediální obraz, odchod klientely.
Provozní	Ztráta možnosti přijímat karty, narušení provozu, výpadky platebních systémů, dohledové dohody.
Interní	Nutnost reorganizace, revize procesů, nové technologie, školení zaměstnanců, krizové řízení.

Zdroj [17]

Z výše uvedeného vyplývá, že dodržování požadavků PCI DSS není formální administrativní povinností, ale strategickým základem pro stabilní a bezpečné fungování v digitálním obchodním prostředí. Organizace, které požadavky ignorují nebo podceňují, vystavují nejen sebe, ale i své zákazníky a partnery výraznému riziku. Naopak firmy, které přistupují k zabezpečení systematicky, získávají důvěru trhu a lepší odolnost vůči současným i budoucím hrozbám.

3. PŘÍPADOVÉ STUDIE: ÚSPĚŠNÉ A NEÚSPĚŠNÉ IMPLEMENTACE PCI DSS V MALOOBCHODĚ

3.1. Případové studie úspěšných implementací

Implementace nejnovější verze PCI DSS 4 představuje v mnoha organizacích nejen technologickou, ale i procesní a kulturní výzvu. Jde o zajištění bezpečnosti platebních údajů od okamžiku, kdy zákazník zadá číslo karty, až po uložení či zaúčtování transakce v interních systémech. Při důsledném přístupu však může být výsledkem nejen formální splnění požadavků, ale především reálné posílení ochrany citlivých dat a zvýšení důvěry zákazníků. Následující dvě studie z praxe ukazují, jak se k tomu postavily globální společnosti s odlišným zaměřením.

Starbucks: Integrace PCI DSS do mobilních a on-line plateb

Kavárenský řetězec Starbucks je už delší dobu synonymem pro rychlé a pohodlné placení pomocí mobilní aplikace [19]. Vzhledem k tomu, že část zákazníků se do poboček prakticky nedostává bez smartphonu v ruce, staly se digitální platby klíčovým pilířem celkové obchodní strategie. S každoročním růstem objemu mobilních transakcí začalo vedení intenzivně řešit otázku, jak zajistit, aby údaje o platebních kartách zůstaly chráněné v souladu s nejpřísnějšími standardy. Přechod na PCI DSS 4 měl pokrýt jak tradiční platební terminály v kavárnách, tak on-line a mobilní kanály [20]. Při zavádění nových opatření sehrála hlavní roli end-to-end šifrování (E2EE) a tokenizace. Starbucks se rozhodl, že reálná čísla karet se v jeho systémech nebudou vůbec uchovávat v čitelné podobě, ale převedou se na speciální tokeny, které nemají žádnou vypovídací hodnotu mimo interní infrastrukturu. Tato strategie se uplatnila napříč celou platební cestou: od momentu, kdy zákazník zaplatí přes aplikaci, až po uložení záznamu transakce na serverech. Zároveň se zavedl Zero Trust přístup, kde žádná část sítě ani žádný uživatelský účet nedostává oprávnění k přístupu k tokenům, pokud pro to není explicitně definované pravidlo. V praxi to znamená precizní segmentaci, jasně nastavené firewallové politiky a velmi striktní správu uživatelských rolí [21].

Protože Starbucks své aplikace i infrastrukturu často aktualizuje, a to i v rámci zavádění nových marketingových kampaní, klíčovou součástí změn se stala integrace bezpečnostních procesů do DevOps. Všechny konfigurační změny (např. pravidla pro API, nastavení přístupů či firewallů) se nyní spravují verzovacími nástroji a při každém nasazení nového kódu automatizované kontroly validují, zda tyto úpravy neporušují bezpečnostní zásady. Tím se podařilo rychle reagovat na případné chyby či zranitelnosti, což bylo důležité pro udržení průběžné shody s PCI DSS 4. Současně proběhla i úprava školicích materiálů pro personál; zaměstnanci v pobočkách se naučili,

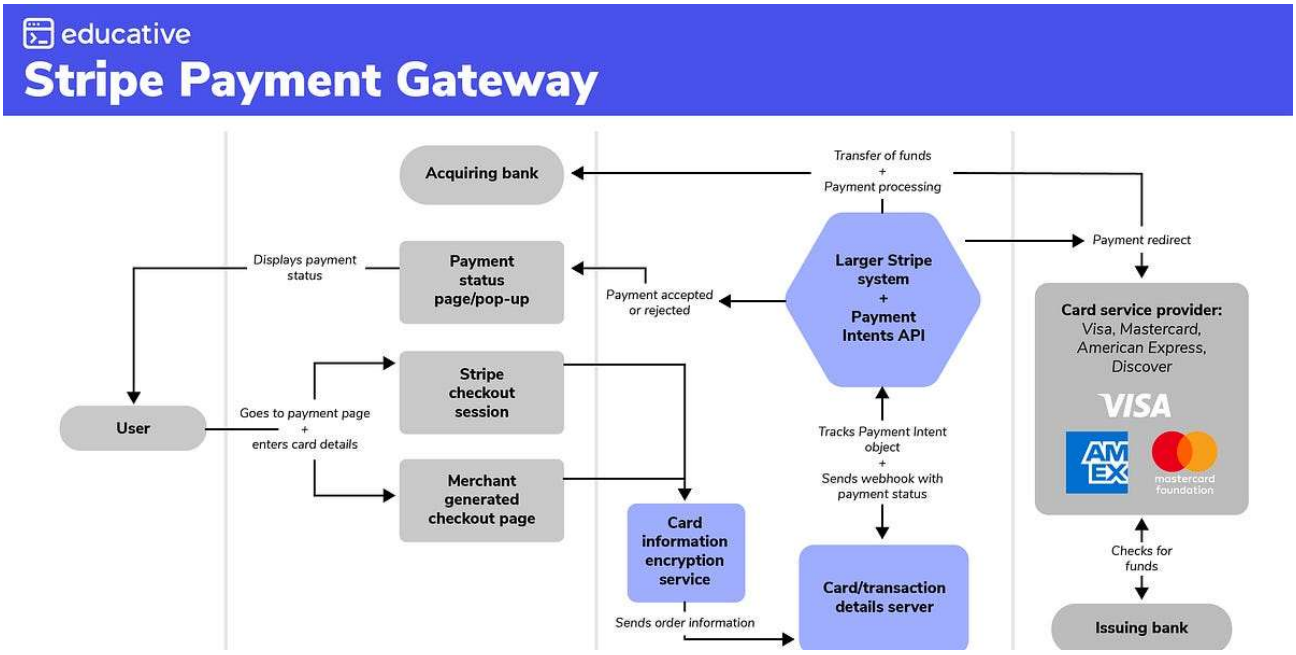
jak reagovat v situaci, kdy mobilní platba selže nebo kdy terminál vykazuje známky neoprávněné manipulace, a IT specialisté zase dostali podrobné postupy pro instalaci šifrovacích klíčů a správu tokenizačních služeb.

Celkovým přínosem pro Starbucks nebylo jen to, že se firma oficiálně sladila s novými požadavky PCI DSS 4, ale hlavně fakt, že dokázala udržet a posílit důvěru u zákazníků, kteří stále více spoléhají na digitální platby. Zavedení tokenizace a nulového ukládání reálných čísel karet minimalizovalo dopady potenciálního úniku dat a integrace bezpečnostních opatření do DevOps procesu podstatně urychlila nasazování nových verzí aplikací.

Stripe: Specializovaný poskytovatel platebních bran pro e-commerce

Stripe je jedním z nejrozšířenějších poskytovatelů internetových plateb pro e-shopy po celém světě. Jeho služby sahají od jednoduchých embedovaných formulářů až po komplexní rozhraní API, která využívají tisíce vývojářů. Od počátku existence kladla společnost důraz na bezpečnost; přesto však přechod na PCI DSS 4 vyžadoval přehodnocení některých interních mechanismů, aby se sladily s důrazem na tokenizaci, detailní logování a řízení přístupových práv. Zásadní roli v této transformaci hrají tzv. vaulty, oddělené úložiště pro reálná čísla karet. Stripe navrhl architekturu, v níž se údaje karet přenášejí po síti výhradně v šifrované formě a končí v bezpečně odděleném „trezoru“, kam mají přístup jen vybrané procesy a silně omezený počet uživatelů. Souběžně byla nasazena pokročilá detekce anomálií v reálném čase, takže pokud nějaký systém začne generovat podezřele vysoký počet zamítnutých plateb nebo opakované pokusy o manipulaci s kartou, vyvolá se okamžité varování [5]. Tato automatizace běží jako doplněk k tradičnímu SIEM nástroji a je přizpůsobená specifickým potřebám e-commerce [22].

Dalším pilířem zabezpečení se stala kombinace penetračních testů (jak interních, tak externích) a bug bounty programu. Stripe se rozhodl aktivně motivovat etické hackery, aby hledali mezery v API a případné chyby v implementacích, za což vyplácí odměny. Díky této strategii dostává společnost zpětnou vazbu mnohem dříve, než by tyto slabiny mohl objevit a zneužít kybernetický útočník. Opravené zranitelnosti se rychle zavádějí do produkčního prostředí – stejně jako v případě Starbucks je zde patrná výrazná vazba na DevOps, protože bezpečnostní změny musejí být plynule integrovány do kódu.



Obrázek 5 Schéma architektury Stripe

Zdroj **[22]**

Velmi důležitou roli hraje i auditní logování každé konfigurace, každého přístupu a každé změny v infrastruktuře. Vše se verzuje a je možné zpětně vysledovat, kdy a kým bylo co upraveno, což výrazně zjednodušuje případné vyšetřování incidentů a je plně v souladu s požadavky PCI DSS 4 na dohledatelnost a archivaci logů. Kromě toho Stripe své zaměstnance průběžně školí v oblasti bezpečnostních pravidel a minimálních oprávnění (least privilege), čímž se dále snižuje pravděpodobnost lidské chyby.

V případě Stripe tak nakonec výsledná podoba vyhovující PCI DSS 4 přinesla zpřísněné procesy pro zpracování karet (tokenizace, oddělené vaulty), nepřetržitý dohled s automatickými upozorněními na anomálie, komplexní auditní záznamy a aktivní spolupráci s komunitou etických hackerů. Tato opatření upevnila pozici společnosti jako spolehlivého partnera pro e-commerce projekty a zároveň poskytla obchodníkům i zákazníkům vyšší míru jistoty, že jejich platební údaje jsou chráněny podle nejnovějších standardů.

Tyto dvě případové studie – Starbucks se zaměřením na mobilní a on-line platby a Stripe jako specializovaná platforma pro e-commerce – ukazují, že přechod na PCI DSS 4 může vypadat různě v závislosti na konkrétním byznys modelu a infrastruktuře. V obou případech však sehrály zásadní úlohu přísná segmentace sítě, tokenizace karet, pokročilé metody šifrování a důsledné zapojení zaměstnanců do bezpečnostního povědomí. Bez ohledu na velikost firmy nebo oblast podnikání se tedy potvrzuje, že úspěšné naplnění nových standardů stojí na kombinaci silných technických

opatření, jasně definovaných postupů a kultury, která vnímá bezpečnost jako kontinuální a společný úkol.

3.2. Případové studie neúspěšných implementací

Přestože organizace často deklarují snahu vyhovět požadavkům PCI DSS, v reálném provozu se někdy ukáže, že formální soulad neodpovídá skutečné úrovni zabezpečení. V této části jsou popsány dvě známé události – zneužití karet ve společnostech Neiman Marcus a Home Depot – které ukazují, že podcenění detailů, zastaralé technologie nebo nejasné definice zodpovědností mohou vést k závažným únikům dat a ztrátě důvěry zákazníků.

Neiman Marcus: Podcenění segmentace a vnitřních procesů

Neiman Marcus, americký řetězec zaměřený na luxusní zboží, se v roce 2013 stal cílem rozsáhlého kybernetického útoku, při kterém došlo k odcizení řady údajů platebních karet. Přestože společnost oficiálně deklarovala dodržování tehdejší verze normy PCI DSS, následné události odhalily několik zásadních nedostatků [23]. Interní analýza ukázala, že segmentace sítě nebyla provedena s dostatečnou důsledností – ač byl formálně vyčleněn samostatný segment pro zpracování karetních transakcí, data se mezi tímto segmentem a ostatními částmi IT infrastruktury přenášela volněji, než vyžadují bezpečnostní předpisy, což umožnilo útočníkům postupně proniknout z méně chráněných oblastí až ke kritickým pokladním systémům.

Dalším problémem bylo nedostatečné logování a monitorování, kdy i přes sběr logů ze zařízení a serverů chyběl jednotný systém pro jejich analýzu, a proto upozornění na podezřelou aktivitu buď nevznikalo, nebo se ztrácelo kvůli absenci centrálního dohledu [24]. Z procesního hlediska se rovněž ukázalo, že formálně deklarovaná shoda s PCI DSS nebyla doprovázena jasným vymezením odpovědnosti – nebylo zřejmé, kdo má incident řešit, komu jej personál hlásit a jakým způsobem má být incident eskalován na vrcholové vedení. Tato nejasnost vedla k pomalé a nekoordinované reakci, což mohlo dále prohloubit vzniklé škody. Následkem incidentu společnost čelila soudním sporům, poklesu důvěry zákazníků a finančním ztrátám, přičemž podrobnější vyšetřování a audity potvrdily, že některé klíčové zásady PCI DSS nebyly dodrženy, ač společnost formálně tvrdila opak. Tento případ tedy jasně dokládá, že formální certifikace sama o sobě nezaručuje skutečnou úroveň zabezpečení, pokud nejsou v praxi řádně implementovány potřebná bezpečnostní opatření a procesy.

Home Depot: Zastaralé systémy a nekonzistentní strategie

Home Depot, jeden z největších severoamerických řetězců pro kutily a stavitele, se v roce 2014 stal terčem jednoho z nejzásadnějších úniků dat týkajících se platebních karet, při kterém útočníci

získali údaje desítek milionů zákazníků. Tento incident měl výrazný dopad na pověst firmy i její hospodářské výsledky a pozdější analýzy ukázaly, že k němu přispělo několik klíčových nedostatků v infrastruktuře a bezpečnostní strategii. Prvním zásadním faktorem byla nekonsolidovaná infrastruktura, kdy různé pobočky provozovaly odlišné pokladní systémy a používaly různé verze softwaru; některé systémy byly značně zastaralé a postrádaly základní funkce šifrování platebních karet. To, že některé pobočky měly centralizovanou správu, zatímco jiné nikoli, vedlo k nejednotnému nasazování bezpečnostních aktualizací a politik, což umožnilo opomenutí klíčových bezpečnostních uzlů. Dále, přestože firma deklarovala oddělení prostředí obsahujícího data držitelů karet od zbytku sítě, v praxi se ukázalo, že síťová segmentace nebyla dostatečně striktní; různé pobočky využívaly různá technická řešení a nebylo vždy jasné, jak jsou propojeny se servery centrály, což útočníkům umožnilo pohybovat se volně vnitřními systémy a přistupovat k zařízení s citlivými informacemi [25] K dalším slabinám patřilo nefunkční monitorování a eskalace událostí, kdy navzdory použití antivirových řešení a nastaveným pravidlům chyběl centralizovaný systém vyhodnocování logů, což vedlo k opožděnému nebo úplnému zanedbání varovných signálů a umožnilo útočníkům delší dobu působit v prostředí firmy. Kritickým momentem byl také nedostatek průběžného školení personálu, kdy zaměstnanci na pobočkách často nevěděli, jak správně reagovat v případě nestandardního chování terminálu, což se projevovalo například při chybách při čtení karet a spoléháním se na rutinní obhlídky bez systematického sledování integrity pokladních zařízení. Jakmile se incident dostal do veřejného povědomí, společnost byla konfrontována s rozsáhlou kritikou, ztrátou důvěry zákazníků, soudními žalobami a přísným dohledem regulátorů.

V reakci na tuto situaci interní týmy ve spolupráci s externími bezpečnostními poradci provedly zásadní reformu, která zahrnovala nahrazení zastaralých systémů, zavedení jednotnější segmentace sítě, implementaci strukturovaného SIEM nástroje a zlepšení školicích programů spolu s jasným vymezením odpovědnosti za provozní bezpečnost a řešení incidentů. Tento případ jednoznačně ukazuje, že nekonzistence v přístupu k bezpečnosti a nedostatečná integrace moderních bezpečnostních opatření mohou mít závažné důsledky pro organizaci.

Společné znaky neúspěšných implementací

Oba příběhy mají několik společných jmenovatelů, které dobře ilustrují, proč se deklarovaná shoda s PCI DSS může v praxi rozpadnout:

- **Formální vs. reálná segmentace**: Příliš mnoho firem považuje segmentaci za splněnou, pokud ji mají na papíře, ale neověřují její faktickou funkčnost. Útočníci pak využijí mezer, jež propojují různé části sítě.

- **Zastaralé nebo nejednotné technologie**: Pokud v jedné polovině poboček běží moderní šifrovací terminály a ve druhé staré neaktualizované systémy, je jen otázkou času, kdy útok proběhne v méně zabezpečeném segmentu.
- **Nejasné kompetence a nedostatečné školení**: V obou případech se ukázalo, že zaměstnanci často netuší, komu mají hlásit incident, co přesně představuje podezřelé chování a kdo za bezpečnost reálně odpovídá.
- **Slabý monitoring a Incident Response**: I když existují logy nebo antivirus, bez správně nastavených procesů a centrálního dohledu zůstávají podezřelé aktivity bez včasné odezvy.

Tyto faktory vedly k velkým finančním ztrátám, poškození reputace a nárůstu nedůvěry u zákazníků. Nejdůležitějším poučením z neúspěšných implementací proto je, že formální plnění standardu PCI DSS nestačí – organizace musejí uvést doporučení do každodenní praxe a soustavně ověřovat, zda nastavená opatření opravdu chrání platební údaje v dynamickém a často velmi komplikovaném provozním prostředí.

4. ANALÝZA STÁVAJÍCÍCH BEZPEČNOSTNÍCH OPATŘENÍ V MALOOBCHODNÍ SÍTI

4.1. Představení společnosti X

Společnost X je předním hráčem na českém maloobchodním trhu, který kromě prodeje potravin a výrobků denní potřeby klade velký důraz na moderní technologie a bezpečnost. Organizační struktura firmy je navržena tak, aby efektivně chránila informační systémy a finanční transakce, což je klíčové pro udržení důvěry zákazníků i obchodních partnerů. Lokální IT oddělení je zodpovědné za správu a údržbu všech informačních systémů společnosti. V jeho rámci funguje specializovaný útvar pro informační bezpečnost, který se stará o ochranu interních dat a bezpečnost platebních transakcí. Tento útvar úzce spolupracuje s dalšími technickými týmy a je připraven rychle reagovat na aktuální kybernetické hrozby, což umožňuje efektivní řešení případných incidentů. Pro zajištění jednotných bezpečnostních standardů a politik společnost X využívá mezinárodní oddělení ISO (INT ISO). Toto oddělení poskytuje odbornou podporu, vypracovává a aktualizuje bezpečnostní směrnice, které jsou implementovány napříč celou organizací. Díky centralizovanému přístupu je zajištěna konzistence a vysoká úroveň ochrany dat ve všech provozovnách společnosti. Další klíčovou složkou je mezinárodní oddělení Payment Security, které se specializuje na zabezpečení platebních transakcí a správu platebních terminálů. Toto oddělení poskytuje podporu nejen společnosti X v České republice, ale také jejím pobočkám v dalších zemích. Díky této mezinárodní podpoře jsou finanční operace prováděny s maximální ochranou, což významně posiluje důvěru zákazníků a obchodních partnerů. Celkově propojení lokálního útvaru informační bezpečnosti, mezinárodního oddělení ISO a mezinárodního oddělení Payment Security umožňuje společnosti X udržovat vysoké standardy ochrany dat a finančních operací, což přispívá k jejímu dlouhodobému úspěchu na trhu.

4.2. Současný stav bezpečnostních opatření

4.2.1. Technologická infrastruktura

Technologická infrastruktura v rámci zkoumané maloobchodní sítě je klíčovým prvkem pro zajištění ochrany platebních údajů i dalších citlivých dat. V současné době je sestavena tak, aby podporovala zpracování velkého objemu transakcí, správu produktových informací a další provozní činnosti typické pro prodejní řetězec s desítkami až stovkami poboček na území České republiky. Současně je částečně propojena s infrastrukturou mateřské společnosti se sídlem v Německu, což vytváří robustní zázemí pro centralizovanou správu a standardizované zabezpečení. V kontextu přípravy na implementaci nové verze PCI DSS je však nezbytné ověřit,

zda každá z klíčových oblastí této infrastruktury – zejména platební terminály, sítě, servery a monitorovací nástroje – splňuje zvýšené bezpečnostní a provozní standardy.

Platební terminály a pokladní systémy

Hlavním prvkem, jenž přímo zprostředkovává platební transakce, jsou moderní POS terminály a pokladní systémy umístěné v každé prodejně. Tyto terminály podporují bezkontaktní i kontaktní platby a jsou centrálně spravovány z důvodu jednotné konfigurace a rychlého nasazování aktualizací (např. bezpečnostních patchů či nových funkcí).

- **Kooperace se servisními centry**: Výměna a údržba terminálů probíhají ve spolupráci se dvěma servisními centry, přičemž konkrétní volba servisního partnera se řídí geografickou polohou pobočky. Rozdělení servisu tímto způsobem zajišťuje rychlou reakci na incidenty či poruchy a zároveň efektivní logistiku náhradních dílů.
- **Výběr na základě auditu ISMS**: Výše zmíněná servisní centra byla vybrána mimo jiné s ohledem na výsledky auditu jejich Systému řízení informační bezpečnosti (ISMS). Dodavatelé musejí splňovat nejen technické a časové požadavky na servis, ale také vysoký standard v oblasti zajištění důvěrnosti a integrity dat.

Z bezpečnostního hlediska hraje klíčovou roli šifrování, které se uplatňuje již na úrovni softwaru terminálu – všechny platební údaje jsou kódovány před samotným odesláním do autorizačního centra. U vybraných systémů je navíc implementována tokenizace, která využívá jednorázových tokenů namísto reálných údajů karty. V případě nutnosti zpětné validace v systému (např. při řešení reklamace transakce) se využívá pouze posledních 4 číslic z karty; celý kód karty se nikde v lokálním prostředí neuchovává, což významně snižuje riziko úniku citlivých dat.

Síťová architektura a segmentace

Síťová architektura je koncipována tak, aby oddělila systémy zpracovávající platební údaje od ostatní podnikové sítě. Tento koncept vychází z principů „nejnižší nutné důvěry“ (tzv. Zero Trust), kde každá podsíť má nastavena přísná pravidla přístupu a je pečlivě monitorována.

- **Segmentace klíčových oblastí**: Prodejny, distribuční centra i administrativní budovy mají oddělené segmenty, přičemž jeden z hlavních segmentů je vyhrazen výhradně pro provoz pokladních systémů a platebních terminálů. V dalších segmentech běží například marketingové systémy, e-mailové servery nebo personalistická agenda.
- **Firewall a IDS/IPS**: Veškerý provoz mezi segmenty je řízen firewallovými pravidly. K detekci podezřelých aktivit či útoků slouží nástroje IDS a IPS, které v reálném čas analyzují

síťový provoz. V případě zachycení anomálií dokážou tyto nástroje automaticky reagovat a zamezit šíření incidentu.

Tento důraz na segmentaci a ochranné mechanismy plyne nejen z obecných principů kybernetické bezpečnosti, ale i z konkrétních požadavků PCI DSS, jež vyžadují například jasné vytyčení tzv. Cardholder Data Environment (CDE) a oddělení od ostatních částí podnikové sítě.

Zobrazeny záznamy 1 až 5 — Transakce - všechny — << < 1 >

Typ transakce	ID Terminálu	ID POS	Datum a čas vzniku	Čas připsání na server	Datum zaúčtování	Stav	Částka	Měna	DCC	Číslo karty/ Číslo účtu	Autoriz. kód	Var. symbol	Vydavatel karty	Zp na ka
Prodej	M1LIDL2711	LIDL2711	28.06.2024 18:52:32	28.06.2024 18:52:46	29.06.2024	Autorizováno/ Zaúčtováno	19.90	CZK		***0233	036475	CS027101761575180241	VISA	L
Prodej	M1LI027181	LI027181	28.06.2024 13:02:18	28.06.2024 13:02:24	29.06.2024	Autorizováno/ Zaúčtováno	19.90	CZK		***7008	952514	CS027181079523180241	VISA	L
Prodej	M1LIDL2712	LIDL2712	28.06.2024 12:01:36	28.06.2024 12:01:52	29.06.2024	Autorizováno/ Zaúčtováno	19.90	CZK		***9350	794507	CS027102849634180241	MASTERCARD	L
Prodej	M1LI027187	LI027187	28.06.2024 11:32:48	28.06.2024 11:32:54	29.06.2024	Autorizováno/ Zaúčtováno	19.90	CZK		***6999	819917	CS027187072432180241	VISA	L
Prodej	M1LI027187	LI027187	28.06.2024 07:00:24	28.06.2024 07:00:29	29.06.2024	Autorizováno/ Zaúčtováno	19.90	CZK		***2236	084870	CS027187072375180241	VISA	L

Obrázek 6 Příklad uložených transakcí v systému

Zdroj: vlastní

Serverová infrastruktura a datová úložiště

V maloobchodní síti existuje několik lokálních datových center v rámci České republiky, která doplňuje serverová infrastruktura mateřské společnosti v Německu. Díky tomuto propojení lze využít centrální zdroje a know-how velké nadnárodní skupiny, přestože se jedná o vlastní servery – provozovatel nevyužívá služby externích cloudových providerů.

- **Hlavní datová centra**: Lokální servery v ČR jsou zodpovědné za klíčové obchodní procesy (např. správu skladových zásob, cenotvorbu, lokální reporting). V zahraniční centrále sídlí mateřské datové centrum s vysokokapacitními storage systémy a robustním zálohováním.
- **Ukládání platebních údajů**: Aby se minimalizovaly nároky na ochranu osobních údajů a splnily požadavky PCI DSS, ukládají se pouze poslední 4 číslice z platební karty. Úplné údaje se v žádném z datových center neshromažďují a k dalšímu zpracování slouží tokenizované záznamy, čímž se snižuje riziko úniku dat a zároveň zjednodušuje auditní proces.
- **Redundance a vysoká dostupnost**: Díky existenci vícero datových center, strategicky rozmístěných v různých regionech, je zajištěna kontinuita provozu i při případném výpadku. Přísné SLA (Service Level Agreements) definují maximální dobu obnovy (RTO – Recovery Time Objective) a cílenou minimální ztrátu dat (RPO – Recovery Point Objective).

Bezpečnostní nástroje a jejich sledování jsou základní součástí technologické infrastruktury. V síti běží systémy, které neustále sledují provoz, hledají neobvyklé aktivity a pomáhají řešit bezpečnostní problémy:

- **SIEM:** Tento systém shromažďuje a analyzuje záznamy z různých zařízení – jako jsou firewally, servery, databáze a pokladní terminály. Díky tomu dokáže včas odhalit neobvyklé chování, což pomáhá předcházet finančním ztrátám a poškození reputace.
- **Integrované bezpečnostní politiky:** Mateřská společnost v Německu stanovila jednotná pravidla a standardy, která platí i pro dceřiné firmy. To znamená, že ve všech zemích se používají stejné postupy pro správu přístupů, dělení sítě a ochranu důležitých systémů.
- **Automatizované reakce a aktualizace:** Kromě sledování provozu jsou k dispozici nástroje, které automaticky distribují bezpečnostní záplaty a aktualizace. Tyto aktualizace se týkají hlavně operačních systémů, antivirových programů a firmware pro pokladní terminály.

Díky těmto opatřením se udržuje stabilní úroveň bezpečnosti v maloobchodní síti a je možné rychle reagovat na nové hrozby. Je však třeba pravidelně kontrolovat účinnost stávajících řešení a přizpůsobovat je novým požadavkům standardů PCI DSS, které dále posilují ochranu zákaznických platebních údajů.

4.2.2. Procesy a politiky ochrany dat

Procesy a politiky ochrany dat v rámci zkoumané maloobchodní sítě vycházejí z centrální bezpečnostní politiky, která je závazná pro všechny pobočky. Tento rámec, připravený mateřskou společností v Německu, reflektuje globální standardy (např. PCI DSS) i vnitrofiremní požadavky na ochranu citlivých informací [15]. Základním cílem těchto zásad je předcházet bezpečnostním incidentům a zároveň efektivně reagovat, pokud k nim dojde. Níže jsou popsány hlavní oblasti, na které se tato politika zaměřuje.

a) Interní směrnice a standardizované postupy

Všechny pobočky v rámci maloobchodní sítě dodržují centrálně definovanou politiku, která stanovuje:

- **Nakládání s citlivými údaji** (platební karty, osobní data zaměstnanců),
- **Povinnosti a úroveň odpovědnosti** pro různé pracovní role a oddělení,
- **Správu a údržbu** informačních systémů a platebních terminálů,
- **Postup při řešení incidentů**, od nahlášení až po konečnou analýzu příčin.

Veškeré tyto postupy jsou jednotně dokumentovány, aby se zachovala konzistence napříč všemi zeměmi, kde společnost působí. Metodiky, které tuto politiku doplňují, rozpracovávají konkrétní technická a procesní témata (např. přístupová práva, segmentace sítě, fyzické zabezpečení a podobně).

b) Pravidelné školení personálu

Všichni zaměstnanci, kteří přicházejí do styku s platebními terminály nebo jinými kritickými systémy, musejí absolvovat každoroční školení [2]. To je strukturováno podle jednotlivých skupin:

1. **Personál prodejen**
    - Praktická obsluha terminálů (řešení technických problémů, rozpoznání neoprávněné manipulace).
    - Bezpečnostní zásady pro každodenní provoz a komunikaci se zákazníky.
    - Postupy při incidentu (nefunkční terminál, podezřelá transakce atp.) – zaměstnanci jsou poučeni, že jakýkoli incident musí být okamžitě hlášen a zadán do ticketovacího systému.
2. **Manažeři prodejen**
    - Odpovědnost za provozní bezpečnost pobočky, koordinace personálu při výskytu incidentu.
    - Komunikace s bezpečnostními složkami a nadřízenými odděleními (např. Service & Support).
    - Řešení eskalací a dozor nad správným dodržováním směrnic.
3. **Pracovníci oddělení Service & Support**
    - Pokročilé znalosti a kompetence pro diagnostiku hardwarových i softwarových závad terminálů.
    - Standardizované postupy ve spolupráci se servisními centry – např. objednávka výměny terminálů, řízení oprav.
    - Bezpečnostní zásady při práci s citlivými komponentami (záznamy transakcí, nastavení pokladních systémů).
4. **IT personál a administrátoři**

- Hlubší technická znalost požadavků PCI DSS, segmentace sítí, správy přístupů a logování.
- Patch management a nasazování bezpečnostních aktualizací.
- Aktivní účast na vyhodnocování kybernetických hrozeb a řešení rozsáhlejších incidentů.

Monitoring účasti a reportování

Interní bezpečnostní oddělení plánuje harmonogram školení, sleduje účast zaměstnanců a vydává pravidelné reporty pro nejvyšší vedení. Díky tomu je zajištěno:

- **Pravidelné proškolení** ve stanoveném termínu,
- **Zachycení případných mezer** ve znalostech,
- **Aktualizace obsahu** podle aktuálních trendů v oblasti kybernetické a provozní bezpečnosti.

c) Re-certifikace a kontrolní audity

Jednou ročně dochází k re-certifikaci, v rámci níž si auditor (interní nebo externí) náhodně vybere přibližně 10 prodejen. Ty jsou podrobeny detailnímu šetření, aby se ověřilo, zda personál skutečně ovládá předepsané bezpečnostní postupy.

Kontrolní otázky pro personál

Během auditu jsou kladeny otázky, které simulují reálné situace:

- „Co uděláte, když terminál přestane fungovat?“
- „Jak a komu hlásíte nefunkční terminál?“
- „Jak se zachováte, pokud zaznamenáte podezření na neoprávněnou manipulaci s terminálem?“

Zaměstnanci by měli umět vysvětlit konkrétní kroky, včetně okamžitého hlášení do ticketovacího systému, aby se informace o incidentu dostala k příslušným týmům v co nejkratším čase.

Vyhodnocení a nápravná opatření

Výsledky auditu slouží k odhalení případných nedostatků v povědomí personálu či v provozních postupech. Pokud kontrola identifikuje slabé místo (např. nejasnosti ohledně toho, kdo je Responsible nebo Accountable podle RACI modelu), vedení přijímá následující opatření:

- **Úprava školicích materiálů** nebo testovacích scénářů,
- **Posílení procesů** hlášení a dokumentace incidentů,
- **Doplnění postupů** v interních směrnicích či operativních pokynech.

d) Kontinuita a rozvoj bezpečnostních politik

Společnost pravidelně reviduje své bezpečnostní politiky a procesy, aby odpovídaly aktuálním verzím normy PCI DSS a změnám v legislativě, například v rámci GDPR. Tento přístup umožňuje pružně reagovat na nové bezpečnostní hrozby a minimalizovat riziko sankcí či poškození reputace. Po každém bezpečnostním incidentu se provádí podrobná retrospektivní analýza, během níž se identifikují nedostatky v procesech a případné zpoždění v hlášení incidentů, což vede k úpravám školících materiálů a interních směrnic.

Velký význam má i spolupráce s mateřskou společností, která přispívá sdílením svých zkušeností a osvědčených postupů na mezinárodní úrovni. Součástí strategického řízení ochrany dat je také budování bezpečnostní kultury napříč celou organizační strukturou, kdy se klade důraz na pravidelnou komunikaci zásad a hodnot bezpečnosti se zaměstnanci, motivaci k včasnému hlášení incidentů bez obav z postihu a na vzájemné sdílení informací mezi odděleními, například mezi IT a obchodním personálem. Díky kombinaci jednotné bezpečnostní politiky, pravidelných auditů, důkladného školení a efektivního systému okamžitého hlášení incidentů se organizace snaží dlouhodobě udržet vysokou úroveň ochrany dat, což je zásadní pro plnění požadavků PCI DSS a dalších mezinárodních norem.

4.3. Identifikace slabých míst v současných procesech

Přestože je v maloobchodní síti nastavena centrální bezpečnostní politika, existuje řada aspektů, které ne zcela odpovídají nejnovějším požadavkům PCI DSS či současným trendům v oblasti informační bezpečnosti. Při podrobnější analýze se ukázalo, že některé z dříve nastavených pravidel nevycházejí z aktuálních rizik a mohou vést k podcenění možných hrozeb [26]. V následujícím textu jsou uvedeny hlavní slabé stránky, které byly identifikovány v rámci prověrky dosavadních procesů.

Nedostatečná frekvence a hloubka interních auditů

Podle zásad PCI DSS je nutné provádět periodické audity, ovšem samotná norma přesně nedefinuje, jak často by se měly konat – tato volba je ponechána na vrcholovém managementu. V posuzované síti se nicméně ukázalo, že dosavadní rozhodnutí o četnosti auditů vychází ze zastaralých interních směrnic, přičemž klíčové parametry nebyly revidovány téměř dvě desetiletí. Konkrétně jde o nastavení, podle nějž má dojít k „auditu“ jednou denně před otevřením pobočky, s následným záznamem v back-office systému. V praxi tato kontrola často probíhá jen jako rychlé ověření, zda jsou pokladní terminály funkční. Nejedná se tedy o skutečný audit, který by reflektoval současnou míru kybernetických rizik, požadovanou hloubku kontroly či aktualizované požadavky PCI DSS. Celý proces tak může vést k mylnému dojmu, že je síť zajištěna dostatečně, přestože mohou zůstat nezjištěny závažné nedostatky. Navíc od vydání původního rozhodnutí došlo k výraznému posunu technologií, standardů i způsobů útoků, a proto by měl být interval a náplň interních auditů znovu důkladně přehodnoceny.

Absence formálního RACI modelu v rutinních postupech

RACI model představuje důležitý nástroj pro vymezení rolí, odpovědností a komunikačních toků. Ačkoli je v některých ohledech (např. při implementaci technických řešení nebo v rámci organizačních projektů) využíván, u rutinních bezpečnostních kontrol a každodenního provozu se uplatňuje spíše neformálně. V řadě případů tak není pevně stanoveno, kdo je skutečně odpovědný (Accountable) za konečný výsledek, kdo má úkol fyzicky vykonat (Responsible), koho je nutno konzultovat (Consulted) a kdo by měl být pouze informován (Informed).

Tato nejednoznačnost se nejzřetelněji projevuje ve chvílích, kdy dojde k incidentu spojenému s platebním terminálem (například technická závada, podezření na manipulaci nebo chybné transakce). Pokud personál v takové situaci netuší, jaké má kompetence a kdy má incident eskalovat, prodlužuje se doba reakce, což může zvýšit škody nebo ohrozit plynulost provozu. Jasně definované RACI by naopak pomohlo zefektivnit koordinaci jednotlivých oddělení, jako je IT, Service & Support či vrcholové vedení.

Nedostatky v praktických testech a simulacích

Ačkoli existuje systém re-certifikace a pravidelných školení, neprobíhají vždy dostatečně hloubkové testy připravenosti. Zaměstnanci sice teoreticky vědí, jak se chovat při výskytu anomálií, avšak v praxi by mohl nastat problém v situacích, které nebyly dostatečně natrénovány v rámci reálných nebo simulovaných scénářů. Následkem toho mohou, zejména v době zvýšené zátěže, zaměstnanci jednat pod tlakem chybně nebo neefektivně. Pro ilustraci lze uvést penetrační

testy, které jsou sice prováděny na úrovni centrální infrastruktury, ale ne vždy zahrnují individuální prodejny. Přitom právě v těchto pobočkách dochází k fyzické manipulaci s platebními zařízeními a stýkají se tam různé kategorie zaměstnanců s rozdílnými kompetencemi.

Slabiny ve spolupráci se servisními partnery

Další oblast, kde lze identifikovat prostor pro zlepšení, se týká procesu předávání podnětů servisním centrům, jež zajišťují výměnu a opravy terminálů. Ačkoliv obě servisní centra prošla úspěšným auditem vlastního ISMS a byla uznána jako bezpečnostně způsobilá, zůstává problémem ne zcela jasně stanovená reakční doba při specifických incidentech, které nejsou rutinní povahy. V případě komplexnějšího incidentu, vyžadujícího součinnost více týmů, se komunikace občas protahuje, protože chybějí jasně formulované servisní smlouvy (SLA) obsahující dohody o eskalačních úrovních a deadliny k odstranění závad.

Neaktualizovaná dokumentace a provozní manuály

V rámci bezpečnostní politiky sice existuje jednotný rámec, který pokrývá klíčové otázky ochrany dat a kybernetické bezpečnosti. Některé konkrétní návody a metodiky na úrovni jednotlivých poboček však vycházejí spíše z historických zkušeností, než aby reflektovaly nejnovější verze korporátních směrnic či požadavky PCI DSS.

To může vést k situacím, kdy se starší dokumentace rozchází s aktuálními doporučeními, což vyvolává zmatek v tom, jaký postup je správný. Některé prodejny si navíc mohou uchovávat vlastní návody k obsluze terminálů či řešení incidentů, které nemusí být plně v souladu se společnou politikou. Takový nesoulad ve vnitřní dokumentaci oslabuje celkovou bezpečnost sítě, jelikož se zaměstnanci orientují podle různých verzí týchž pravidel.

Možné dopady a rizika plynoucí z nedostatků

Z uvedených slabých stránek vyplývá, že současné nastavení procesů by mohlo ve výsledku vést k několika reálným rizikům. Především hrozí, že potenciální útok či technická zranitelnost zůstanou bez povšimnutí, nebo budou odhaleny až příliš pozdě. Nedostatečná hloubka auditů nemusí zachytit známky narušení, zatímco absence jasně definovaného RACI modelu může vést ke zbytečným průtahům, než se podaří problém vyřešit.

V rychle se rozvíjejícím světě digitálních plateb je včasná reakce a odhalení incidentu naprosto zásadní, ať už jde o ochranu citlivých dat zákazníků či zajištění plynulého provozu celé maloobchodní sítě. Aktuální frekvence auditů stanovená před více než dvaceti lety rozhodně neodráží moderní nároky na kybernetickou bezpečnost. Přestože se každý den formálně provádí kontrola a zápis do systému, ve skutečnosti tato procedura nepokrývá všechny nutné aspekty.

Současná praxe by se proto měla přizpůsobit novým požadavkům a hrozbám, a to jak v oblasti pravidelných, skutečně hloubkových auditů, tak při vymezení zodpovědností a eskalačních procesů. Bez těchto úprav se vystavuje síť riziku finančních ztrát, reputačního poškození a případných sankcí za nesoulad s PCI DSS či dalšími mezinárodními normami.

5. OPTIMALIZACE PROCESŮ PRO SPLNĚNÍ POŽADAVKŮ PCI DSS

5.1. Metodologie analýzy procesů

Při přechodu z předchozí verze PCI DSS 3.5 na verzi 4 je zásadní prověřit, do jaké míry stávající procesy reálně vyhovují novým či upraveným požadavkům standardu. V rámci rozsáhlého maloobchodního prostředí, kde každodenně dochází ke zpracování obrovského množství platebních transakcí, je přitom nutné zohlednit nejen technické náležitosti (například segmentaci sítě, šifrování či monitorování logů), ale i organizační a personální faktory. Právě ty často rozhodují, zda se deklarované postupy skutečně uplatňují, nebo zůstávají jen formálně zapsané v interních předpisech [6].

Úvodním krokem je pečlivé vymezení rozsahu analýzy (tzv. scoping). V této fázi je nezbytné definovat, které části infrastruktury a které procesy spadají pod tzv. Cardholder Data Environment (CDE). Do CDE obvykle patří nejen systémy přímo zacházející s kartovými údaji (platební terminály, pokladní systémy, databáze transakcí), ale i navazující podpůrné a administrativní činnosti. Praktická zkušenost ukazuje, že v maloobchodní síti je často komplikované toto prostředí skutečně oddělit, protože některé „technické zkratky“ (např. sdílené servisní účty, vzdálená správa či integrační skripty) mohou hranice CDE výrazně narušovat [27]. V této souvislosti je rovněž nutné zohlednit nejnovější požadavky PCI DSS 4, které kladou větší důraz na detailní popis komunikačních toků a na tzv. targeted risk analysis pro specifické scénáře. Po vymezení rozsahu následuje detailní zmapování reálného fungování organizace. K tomu se často využívají workshopová sezení s pracovníky na různých úrovních – od obsluhy pokladen, která řeší každodenní manipulaci s terminály, až po IT a bezpečnostní specialisty, kteří spravují serverovou infrastrukturu a nastavují přístupové politiky. Na těchto setkáních se krok za krokem popisuje, co se reálně děje s platbou od chvíle, kdy zákazník přiloží či protáhne kartu, přes autorizaci transakce, až po zaúčtování a archivaci. Cílem je odhalit i zdánlivě banální rutiny, které ale mohou mít zásadní dopad na bezpečnost. Typickým příkladem bývá dočasné ukládání výpisů či logů v nešifrované formě nebo improvizované „zálohy“ vytvářené lokálně na pobočce. Součástí analýzy je následné vyhodnocení, kde a v jaké podobě dochází k manipulaci s reálnými kartovými údaji. PCI DSS 4 v některých bodech dále zpřísňuje požadavky na tzv. data minimization, tj. minimalizaci ukládání či zpracovávání citlivých informací. Pokud se například ukáže, že určité oddělení nepotřebuje znát celé číslo karty a postačí mu pouze poslední čtyři cifry pro účely reklamací, lze uvažovat o nasazení tokenizace či dalších metod, které snižují riziko v případě úniku dat. V této fázi se zjišťuje, zda je vhodné využít modernizaci pokladních systémů

nebo nasadit platformu pro centralizované zpracování a správu klíčů (KMS), která by byla v souladu s novými ustanoveními standardu. Na základě procesního modelu se provádí analýza rizik, jež zohledňuje všechny identifikované úkony a potenciální slabá místa. Při přechodu z předchozí verze na PCI DSS 4 se často ukáže, že některé dříve akceptovatelné kompromisy či „lokální výjimky“ (například slabší segmentace sítě v menších pobočkách nebo používání sdíleného servisního hesla pro rychlou údržbu) již nelze nadále tolerovat. K posouzení rizik je možné využít matice kombinující pravděpodobnost výskytu a dopad incidentu: vysoká rizika pak dostávají prioritu pro odstranění, zatímco nižší rizika lze řešit v dalších fázích.

Důležitou etapou je tzv. gap analysis [6], tedy srovnání zjištěného stavu s konkrétními body standardu. Zatímco PCI DSS 3.5 mohla tolerovat určité scénáře, verze 4 často zavádí přísnější požadavky nebo vyžaduje doložit, že bylo provedeno konkrétní rizikové vyhodnocení. To může znamenat např. nutnost jasně prokázat, proč je určitý typ šifrovacího algoritmu či konkrétní metodika segmentace považována za dostatečnou. Výsledkem gap analysis je obvykle přehledná tabulka nedostatků s uvedením, jaká opatření (technická, organizační či procesní) jsou potřebná k jejich odstranění. Dalším krokem je návrh a postupné zavádění konkrétních zlepšení. Někdy stačí menší zásah, například úprava nastavení firewallu či přidání dvoufaktorové autentizace pro vzdálený přístup, jindy je nutné zavést robustní řešení – nasadit nový SIEM (Security Information and Event Management) pro centralizovaný dohled nebo předefinovat procesy pro eskalaci incidentů. Tento krok by měl probíhat v úzké spolupráci s manažery poboček i IT týmem, aby byla zajištěna reálná proveditelnost a aby se eliminovalo riziko, že nově nastavená pravidla nebudou přijata pracovníky v terénu. Při větších změnách, například při kompletním předělání pokladní infrastruktury, je vhodné plán rozdělit na menší fáze a pilotní projekty, které umožní postupně ověřovat funkčnost a dolaďovat detaily. Poslední fáze metodologie analýzy procesů se věnuje kontrole úspěšnosti zavedených opatření. Doporučuje se provádět pravidelné interní audity nebo penetrační testy, které ověří, zda nově definované procesy a technologie odpovídají formálním požadavkům PCI DSS 4 i reálné praxi. Současně je vhodné vyhodnocovat zpětnou vazbu od personálu, jenž s novými postupy pracuje, a aktualizovat interní směrnice podle toho, jak se mění situace na pobočkách. Důležité je rovněž průběžně sledovat vývoj kybernetických hrozeb a regulačních požadavků, protože PCI DSS 4 nemusí být poslední významnou aktualizací – v dynamickém maloobchodním prostředí lze předpokládat, že přijdou další změny, které budou klást nové nároky na infrastrukturu a procesy.

Celá metodologie tak stojí na několika pilířích: přesném vymezení rozsahu (kde a jak se manipuluje s citlivými údaji), realistickém procesním modelování (zachycení denní praxe, nikoli jen formálních směrnic), důkladné analýze rizik s důrazem na novinky ve verzi 4, pečlivém

gap analysis a postupném zavádění opatření s následnou kontrolou. Pouze komplexní a důsledný přístup dokáže zajistit, aby se přechod na PCI DSS 4 nestal pouhou formální záležitostí, ale skutečně vedl k zvýšené úrovni bezpečnosti karetních dat a k udržení důvěry zákazníků.

5.2. Návrh optimalizovaných postupů

Na základě výsledků Protokolu o provedení analýzy rizik a zjištěných slabých míst v bezpečnostních procesech maloobchodní sítě je nutné navrhnout konkrétní optimalizační opatření, která zajistí plnou shodu s požadavky PCI DSS 4. Návrh se zaměřuje na odstranění identifikovaných nedostatků, zejména v oblasti provozních postupů, spolupráce se servisními partnery a interních auditů, které jsou klíčové pro zajištění kontinuálního zlepšování bezpečnostní úrovně. Během analýzy bylo odhaleno několik klíčových problémů, které představují potenciální rizika pro bezpečnost zpracování platebních údajů. Mezi nejvýznamnější patří [16]:

- **Neaktualizovaná dokumentace a provozní manuály**
- **Slabiny ve spolupráci se servisními partnery**
- **Nedostatky v praktických testech a simulacích**
- **Absence formálního RACI modelu v rutinních postupech**
- **Nedostatečná frekvence a hloubka interních auditů**

Optimalizační návrh se proto soustředí na tři hlavní oblasti: posílení interních auditů, zavedení aplikace pro řízení auditních záznamů a formální zavedení RACI modelu v každodenních postupech. Jedním z nejdůležitějších opatření je modernizace systému interních auditů, která zahrnuje nejen zvýšení frekvence auditů, ale také zavedení hloubkových kontrol zaměřených na praktické prověřování postupů práce s platebními terminály. Současná praxe provádění auditů jednou ročně neodpovídá požadavkům PCI DSS 4, který klade důraz na průběžné a systematické vyhodnocování bezpečnostních opatření. Navržený auditní plán zahrnuje pravidelné kontroly zaměřené na každodenní činnosti personálu a simulace reálných incidentů, které mají za cíl prověřit schopnost zaměstnanců správně reagovat na bezpečnostní problémy.

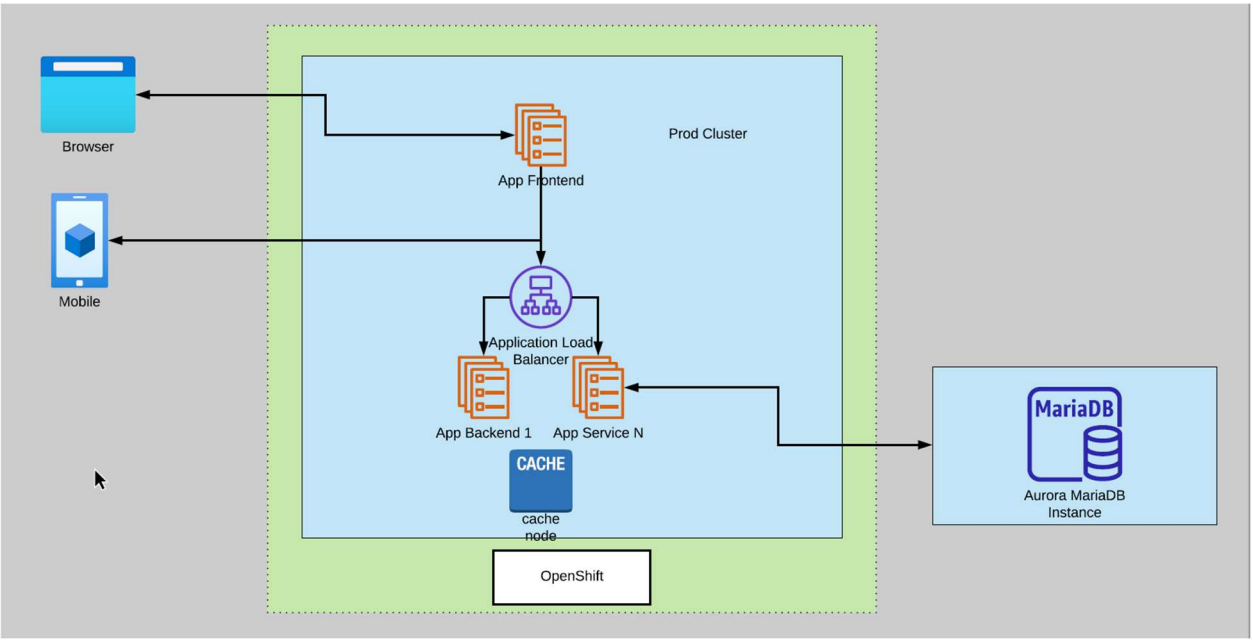
Jedním z klíčových opatření je modernizace procesu kontroly platebních terminálů. Původní postup zahrnoval každodenní manuální kontrolu terminálů personálem na pobočkách, přičemž výsledky této kontroly byly následně zadávány do back-office systému. Tento proces byl časově náročný, náchylný k chybám a neumožňoval okamžité ověření správnosti zadávaných dat. Navíc

byla frekvence kontrol určena před více než 20 lety a nebyla průběžně aktualizována podle aktuálních bezpečnostních rizik.

Tento přístup eliminuje potřebu ručního zadávání dat do systému a zároveň zvyšuje přesnost a rychlost kontroly. Každý terminál bude opatřen jedinečným čárovým kódem, který bude obsahovat informace o jeho sériovém čísle, datu poslední kontroly a stavu plomb.

Proces kontroly bude probíhat následovně:

1. Zaměstnanec obdrží handheld zařízení s nainstalovanou aplikací.
2. Aplikace ho provede jednotlivými kroky kontroly, včetně skenování čárového kódu na plombě terminálu.
3. Aplikace automaticky ověří, zda jsou plomby neporušené, a záznam o kontrole se okamžitě uloží do centrální databáze.
4. V případě zjištění nesrovnalostí (poškozená plomba, chybějící terminál) aplikace automaticky vygeneruje incident, který bude eskalován na centrální IT podporu



Obrázek 7 Schéma aplikace pro kontrolu terminálů

Zdroj [6]

Frekvence těchto kontrol bude nově určena na základě hodnocení rizik prováděného vedením organizace. Top management bude povinen pravidelně přehodnocovat aktuální rizika a na jejich základě stanovit optimální frekvenci kontrol terminálů. Tento přístup umožňuje flexibilně reagovat na změny v prostředí kybernetických hrozeb a přizpůsobovat bezpečnostní opatření aktuálním potřebám. Dalším krokem je zavedení formálního RACI modelu pro klíčové provozní

postupy. Analýza rizik odhalila, že v současné praxi často chybí jasné definování odpovědností a pravomocí při řešení běžných provozních problémů, což vede k prodlevám v řešení incidentů a neefektivní komunikaci mezi jednotlivými odděleními. RACI model umožňuje přiřadit každému procesu konkrétní odpovědné osoby, což zlepšuje transparentnost a usnadňuje řešení nečekaných situací. Například při výpadku platebního terminálu je nyní jasně stanoveno, kdo je zodpovědný za inicializaci opravy (Responsible), kdo musí schválit následné kroky (Accountable), kdo může poskytovat podporu (Consulted) a kdo musí být o incidentu informován (Informed). Zavedení tohoto modelu pomáhá minimalizovat riziko lidské chyby a zajistit, že každý bezpečnostní problém bude řešen v co nejkratším čase. Frekvence těchto kontrol bude nově určena na základě hodnocení rizik prováděného vedením organizace. Top management bude povinen pravidelně přehodnocovat aktuální rizika a na jejich základě stanovit optimální frekvenci kontrol terminálů. Tento přístup umožňuje flexibilně reagovat na změny v prostředí kybernetických hrozeb a přizpůsobovat bezpečnostní opatření aktuálním potřebám.

Dále je nutné zaměřit se na zlepšení spolupráce se servisními partnery. Během analýzy bylo zjištěno, že výběr servisních center, která zajišťují výměnu a údržbu platebních terminálů, nebyl v minulosti vždy doprovázen důkladným ověřením jejich bezpečnostních standardů. Navrhuje se proto zavedení pravidelného hodnocení servisních partnerů na základě jejich souladu s požadavky PCI DSS a interních bezpečnostních zásad organizace. Toto hodnocení bude prováděno formou pravidelných auditů zaměřených na bezpečnost jejich informačních systémů a postupů při manipulaci s platebními terminály. Optimalizované postupy také zahrnují pravidelné aktualizace provozní dokumentace a manuálů pro personál. Během analýzy bylo zjištěno, že některé pokyny nejsou aktuální a nereflektují nové bezpečnostní požadavky. Aktualizace dokumentace musí probíhat v pravidelných intervalech a musí být zahrnuta jako součást interních auditů. Personál musí mít přístup k aktuálním verzím manuálů, které obsahují podrobné pokyny pro bezpečné zacházení s platebními terminály a řešení incidentů. Navrhovaná optimalizace procesů přinese zvýšení bezpečnostní úrovně celé maloobchodní sítě. Modernizace systému auditů a zavedení aplikace pro evidenci výsledků zajistí lepší dohled nad bezpečnostními opatřeními, zatímco zavedení RACI modelu a zlepšení spolupráce se servisními partnery pomohou minimalizovat riziko lidských chyb a bezpečnostních incidentů. Pravidelné aktualizace provozní dokumentace zajistí, že personál bude vždy pracovat podle aktuálních bezpečnostních standardů. Optimalizace postupů je klíčovým krokem pro zajištění dlouhodobého souladu s PCI DSS 4 a zvýšení důvěry zákazníků v bezpečnost zpracování jejich platebních údajů.

6. IMPLEMENTACE NÁPRAVNÝCH OPATŘENÍ

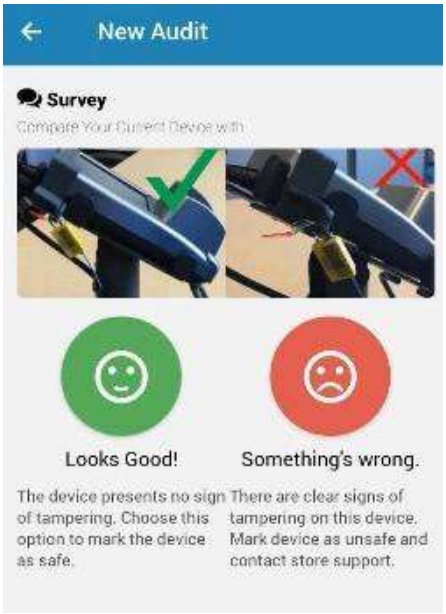
6.1. Aktualizace dokumentace a provozních manuálů

6.1.1. Provozní manuály k platebním terminálům a pokladním systémům

V rámci aktualizace provozní dokumentace byla provedena detailní revize stávajících manuálů vztahujících se k obsluze platebních terminálů a pokladních systémů. Tyto dokumenty vycházely převážně z historických verzí interních směrnic a částečně postrádaly konkrétní pokyny odpovídající aktuálním požadavkům standardu PCI DSS 4.0 [28]. Revize byla zaměřena na doplnění chybějících bezpečnostních opatření, zpřesnění popisů jednotlivých úkonů a sladění terminologie s platnou regulací. Na základě zjištěných nedostatků byl připraven návrh úprav, který zahrnoval následující konkrétní kroky:

Doplnění postupu pro ověřování plomb

Do provozních manuálů byly začleněny detailní pokyny pro fyzickou kontrolu plomb před otevřením provozovny. Nově definovaný postup zahrnuje vizuální kontrolu, porovnání čárového kódu, identifikaci případného narušení a přesný popis eskalačního postupu v případě zjištěné nesrovnalosti. Součástí úpravy jsou také fotografické příklady správně a nesprávně aplikovaných plomb, které slouží jako praktická pomůcka pro personál při každodenním provádění kontrol.



Obrázek 8 Příklad vizuální kontroly plomby před zahájením provozu

Zdroj: vlastní

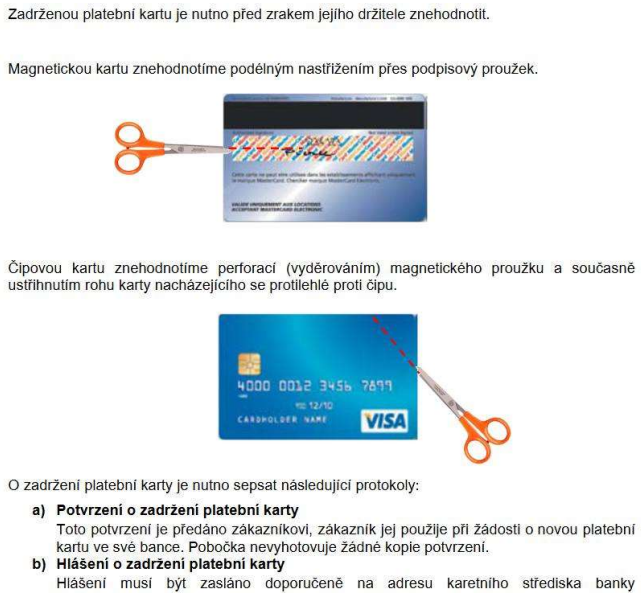
Zavedení pravidel pro kontrolu zobrazovaných údajů

Na základě nových požadavků standardu PCI DSS 4.0 došlo k úpravě instrukcí týkajících se ověřování správného maskování citlivých údajů. Byla stanovena povinnost personálu zkontrolovat, že na účtence ani na obrazovce platebního terminálu nejsou zobrazena jiná data než poslední čtyři číslice platební karty. Tento požadavek byl zároveň začleněn do checklistu pro každodenní rutinní kontroly.

Standardizace postupu při nestandardních situacích s platební kartou

V rámci aktualizace provozních manuálů byl navržen a implementován standardizovaný postup pro řešení situací, kdy dojde k technickým nebo podezřelým problémům během platební transakce. Cílem tohoto opatření je zajistit jednotnou reakci personálu napříč všemi prodejnami a zároveň minimalizovat riziko lidské chyby či bezpečnostního incidentu. Mezi definované scénáře patří například:

- **Karta zůstala v terminálu nebo byla zadržena** Personál je povinen zkontrolovat terminál, neprodleně informovat zákazníka a eskalovat případ na technickou podporu. Pokud není možné kartu vrátit, spouští se bezpečnostní protokol a kontaktuje se servisní partner.



Obrázek 9 Ukázka postupu při zadření karty

Zdroj: vlastní

- **Karta není rozpoznána nebo opakovaně selže platba** Byly přidány pokyny pro opakovaný pokus s jiným způsobem platby (např. kontaktní vs. bezkontaktní),

a následné kroky v případě, že terminál neodpovídá (včetně restartu a hlášení přes ticketovací systém).

- **Podezření na podvod (např. modifikovaný terminál, neautorizované zařízení)** Do manuálu jsem vložil pokyny, jak ověřit fyzický stav zařízení (plomby, vizuální kontrola PINpadu) a jak incident bez prodlení eskalovat. Zároveň byl zaveden jednoduchý formulář pro interní zaznamenání události.
- **Zákazník tvrdí, že platba proběhla, ale terminál transakci nepotvrdil** Byl přidán krokový návod pro ověření transakce v back-office systému a komunikaci se zákazníkem. V případě nejasností je transakce dočasně označena a předána k ověření centrálnímu týmu.

6.1.2. Školící materiály pro personál

V rámci procesu implementace požadavků nové verze standardu PCI DSS 4.0 jsem se zaměřil nejen na technická a organizační opatření, ale i na lidský faktor, který představuje jednu z nejčastějších příčin bezpečnostních incidentů. Nedílnou součástí tohoto procesu proto byla systematická revize a následná aktualizace školících materiálů pro zaměstnance, kteří přicházejí do styku s platebními terminály, pokladními systémy a citlivými údaji držitelů platebních karet. Cílem této aktivity bylo zajistit, že veškerý personál bude nejen teoreticky obeznámen s požadavky PCI DSS 4.0, ale především prakticky připraven reagovat na standardní i nestandardní situace v souladu s aktuálními bezpečnostními postupy.

Původní školící dokumentace vycházela z požadavků starších verzí normy a neobsahovala dostatečně podrobné návody pro nově zavedené prvky, jako je např. kontrola integrity plomb prostřednictvím mobilní aplikace, standardizované eskalační schéma při podezření, na bezpečnostní incident nebo nové pravidlo pro maskování údajů na účtence. Vzhledem k tomu, že některé z těchto změn přímo ovlivňují každodenní provozní činnost zaměstnanců na prodejní ploše, bylo nezbytné přizpůsobit školící materiály tak, aby byly srozumitelné, přehledné a především prakticky použitelné. Proces aktualizace školení začal analýzou stávajících dokumentů, jejichž struktura často neodpovídala potřebám jednotlivých pracovních rolí. Na základě této analýzy jsem vytvořil novou koncepci školení, která zahrnuje rozdělení obsahu podle kompetencí – samostatné moduly byly vytvořeny pro obsluhu pokladen, vedoucí prodejen, pracovníky zákaznické podpory a IT administrátory. Každý modul obsahuje relevantní informace v rozsahu odpovídajícím dané pracovní pozici, přičemž zvláštní důraz byl kladen na provozní realitu v maloobchodním prostředí.

U personálu obsluhujícího terminály byl kladen důraz na rozpoznání fyzických známek manipulace s terminálem (např. poškozené nebo chybějící plomby), schopnost nahlásit incident prostřednictvím interního systému a správnou reakci v případě, že terminál nevykazuje očekávané chování (např. nezobrazí potvrzení o transakci nebo tiskne celé číslo karty). U vedoucích pracovníků byl rozšířen obsah školení o část věnovanou eskalačním schématům, odpovědnosti za rozhodnutí o uzavření terminálu a komunikaci se servisními partnery.

Školící materiály byly připraveny ve více formátech – kromě tištěné verze byla vytvořena i digitální podoba, která byla integrována do interního e-learningového systému společnosti. V rámci digitální platformy jsem navrhl doplnění instruktážních videí pro klíčové procesy, jako je ověření čárového kódu na plombě, použití mobilní aplikace pro kontrolu terminálu nebo simulace reakce na podezřelou transakci. Pro ověření pochopení obsahu byly do každého modulu začleněny kontrolní otázky a testové scénáře, které slouží nejen jako opakovací prvek, ale i jako nástroj k vyhodnocení úspěšnosti školení. Zvláštní pozornost jsem věnoval zpětné vazbě od účastníků. Po každém školení byly distribuovány krátké dotazníky zaměřené na srozumitelnost, přehlednost a užitečnost školeného obsahu. Na základě vyhodnocení odpovědí byly provedeny drobné úpravy textů, především v oblasti jazykové jednoduchosti, vizuální orientace v dokumentech a přehledného členění informací. Aktualizované školení tak představuje významný posun oproti předchozímu stavu. Zajišťuje, že personál nejen rozumí tomu, co se od něj očekává v konkrétních situacích, ale také že ví, jak správně jednat bez nutnosti improvizace. Díky tomuto kroku došlo ke zvýšení připravenosti zaměstnanců a současně k posílení bezpečnostní kultury v celé maloobchodní síti. Tento přístup je v plném souladu s požadavky PCI DSS 4.0 [29], které kladou důraz nejen na technické zabezpečení, ale i na informovanost a školení lidských zdrojů.

Tabulka 2 Rozdělení obsahu školení podle rolí zaměstnanců

Role zaměstnance	**Klíčová témata školení**	**Cíl školení**
Pokladní personál	- Kontrola plomb - Správné zobrazení údajů na účtence - Reakce na nestandardní situace	Zajistit, aby obsluha rozpoznala a správně řešila incidenty
Vedoucí prodejny	- Eskalační schéma - Komunikace se servisním partnerem - Interní reportování	Umožnit efektivní řízení incidentů a odpovědnost
Zákaznická podpora	- Práce s informacemi o transakcích - Interní dokumentace incidentů - Práce s logy	Zajistit podporu prodejen při reklamaci a analýze chyb

IT administrátoři	- Přístupová práva - Monitorování systému - Práce s aplikací a logy	Udržovat technické zázemí v souladu s požadavky PCI DSS

Zdroj: vlastní

6.2. Posílení spolupráce se servisními partnery

6.2.1. Identifikace kritických partnerů

Jako výchozí krok při návrhu systému řízení dodavatelů jsem provedl podrobnou identifikaci kritických partnerů, kteří mají přímý nebo nepřímý vliv na bezpečnostní architekturu prostředí CDE (Cardholder Data Environment). Tato aktivita byla motivována požadavky normy PCI DSS 4.0, konkrétně oddíly týkajícími se řízení třetích stran [26], které se podílejí na zpracování, přenosu nebo ukládání údajů držitelů platebních karet, případně mají přístup k technologiím, které tuto činnost zprostředkovávají.

Nejprve jsem provedl mapování všech externích subjektů, které vstupují do provozu v rámci obchodní sítě společnosti. K tomu jsem využil dostupné databáze smluv, servisních záznamů a ticketovacích systémů, kde je evidována veškerá interakce mezi společností a jejími dodavateli. Dále jsem analyzoval procesní modely a provozní dokumentaci, abych zjistil, které činnosti jsou zajišťovány interně a které naopak prostřednictvím externích subjektů.

Na základě této analýzy jsem definoval tři hlavní kritéria pro označení partnera jako „kritického“:

1 Fyzický přístup ke komponentám infrastruktury CDE – například servisní technici, kteří provádějí výměnu nebo údržbu platebních terminálů.
2 Přístup k systémovým konfiguracím nebo datům prostřednictvím vzdálené podpory – například partneři, kteří poskytují technickou asistenci nebo diagnostiku na dálku.
3 Přímý dopad na funkčnost nebo dostupnost systémů zpracovávajících transakce – například poskytovatelé komunikačních kanálů nebo pokladních softwarových řešení.

Podle výše uvedených kritérií byli jako kritičtí partneři identifikováni především dva servisní partneři, kteří zajišťují údržbu a výměnu platebních terminálů v celé síti prodejen. Tito partneři byli původně vybráni na základě geografického rozdělení a historických referencí, přičemž jejich výběr proběhl před zavedením současného rámce pro řízení rizik dodavatelů. V rámci procesu přechodu na PCI DSS 4.0 však bylo nezbytné posoudit jejich činnost z pohledu bezpečnosti, souladu s normami a úrovně dokumentace poskytovaných služeb. Identifikace těchto subjektů jako bezpečnostně významných byla důležitá pro zahájení následujících kroků, jako je hloubkové posouzení jejich bezpečnostní způsobilosti, doplnění smluv o příslušné bezpečnostní klauzule,

stanovení reakčních lhůt, zavedení povinných pravidelných auditů a definování přesných postupů při incidentu [6]. Zároveň bylo nutné vyhodnotit, zda mají tito partneři zaveden vlastní ISMS (Information Security Management System) a zda je možné jejich vnitřní bezpečnostní procesy považovat za dostatečné z hlediska požadavků PCI DSS. Tímto krokem byla vytvořena základna pro systematické řízení dodavatelů, založené na konkrétních rizicích a provázanosti jejich činností s provozem obchodní sítě. Zvolený přístup umožnil nejen lépe pochopit rizika spojená s externími vstupy do prostředí CDE, ale i připravit půdu pro zavedení standardizovaného modelu „supplier governance“, který bude součástí interní bezpečnostní politiky společnosti.

6.2.2. Analýza smluv a návrh bezpečnostních očekávání

Po identifikaci kritických partnerů jsem se zaměřil na podrobnou analýzu smluvních vztahů mezi společností a těmito dodavateli. Cílem této části bylo ověřit, zda stávající smlouvy a přidružené dokumenty (např. SLA – Service Level Agreements) zohledňují bezpečnostní aspekty vyžadované standardem PCI DSS 4.0, a případně navrhnout jejich úpravu nebo doplnění.

Prohlášení o bezpečnosti informací a ochraně osobních údajů

1.1-1 Informationssicherheitsrichtlinien müssen über einen verbindlichen Vorgaben-Management-Prozess dokumentiert, freigegeben und an relevante Gruppen kommuniziert werden. Zusätzlich müssen diese regelmäßig hinsichtlich Eignung und Angemessenheit überprüft werden.	1.1-1 Zásady bezpečnosti informací jsou zdokumentovány, schváleny a sděleny příslušným skupinám prostřednictvím závazného procesu říz zásad. Kromě toho jsou pravidelně přezkoumává hlediska vhodnosti a přiměřenosti.
☐ Ja ☐ Nein ☐ teilweise (bitte kommentieren) ☐ nichtzutreffend (bitte kommentieren) Kommentar: hier kommentieren...	☐ ano ☐ ne ☐ částečně (uveďte prosím komentář) ☐ nepoužije se (uveďte prosím komentář) Komentář: zde prosím uveďte komentář...
1.2-1 Informationssicherheitsrollen und -verantwortlichkeiten müssen definiert und entsprechenden Personen zugeordnet werden.	1.2-1 V oblasti bezpečnosti informací jsou jasně definovány role a odpovědnosti a následně jsou přiděleny příslušným osobám.
☐ Ja ☐ Nein ☐ teilweise (bitte kommentieren) ☐ nichtzutreffend (bitte kommentieren) Kommentar: hier kommentieren...	☐ ano ☐ ne ☐ částečně (uveďte prosím komentář) ☐ nepoužije se (uveďte prosím komentář) Komentář: zde prosím uveďte komentář...
1.3-1 Informationssicherheitsrichtlinien für Anwender müssen definiert und an die Anwender kommuniziert werden.	1.3-1 Jsou definovány pokyny pro zabezpečení informací a dále jsou komunikovány uživatelům.
☐ Ja ☐ Nein ☐ teilweise (bitte kommentieren)	☐ ano ☐ ne ☐ částečně (uveďte prosím komentář) ☐ nepoužije se (uveďte prosím komentář)

Obrázek 10 Výřez ze smluvní přílohy – bezpečnostní dodatek

Zdroj: vlastní

Analýza zahrnovala posouzení následujících oblastí:

- formální vymezení rozsahu poskytovaných služeb ve vztahu k provozu zařízení, která zpracovávají nebo přenášejí platební údaje;

- reakční časy při výskytu provozních nebo bezpečnostních incidentů;
- způsob eskalace technických problémů a stanovení zodpovědných kontaktních osob;
- dokumentace o zacházení s citlivými komponentami (např. terminály, datové konektory, firmware);
- ochrana dat, šifrování, autentizace techniků a uchovávání logů o zásazích.

Z provedené analýzy vyplynulo, že některé smluvní dokumenty byly formulovány obecně a nevěnovaly se detailně otázkám bezpečnosti, zejména pokud šlo o neplánované zásahy do systémů nebo výměny zařízení mimo pravidelnou údržbu. V několika případech chyběla zmínka o požadavku na evidenci servisních činností, což znesnadňuje auditní dohledatelnost, jež je však klíčová pro splnění požadavků PCI DSS. Dále nebyly vždy jasně popsány reakční doby při bezpečnostním incidentu, a to včetně způsobu komunikace se zákaznickou podporou nebo IT oddělením provozovatele. Na základě identifikovaných nedostatků byla navržena aktualizace smluvních ujednání v několika oblastech. V první fázi byl vytvořen soubor minimálních bezpečnostních požadavků, které je nutné smluvně zakotvit ve vztahu k partnerům s přístupem k platebním terminálům a pokladním systémům. Mezi tyto požadavky patří například povinnost vést záznamy o servisních zásazích, využívat šifrované komunikační kanály při dálkové správě, pravidelně školit techniky v oblasti bezpečnosti a doložit jejich odbornou způsobilost. Dále bylo doporučeno doplnění části SLA o mechanismus eskalace. Nově navržené vícestupňové eskalační schéma definuje konkrétní reakční časy (např. do 1 hodiny při výpadku více než jednoho terminálu na pobočce), role jednotlivých stran a související dokumentační povinnosti. Cílem tohoto opatření je eliminace zpoždění v důsledku nejasného vymezení odpovědnosti mezi interním IT a externím dodavatelem. Součástí návrhu je také bezpečnostní dodatek ke smlouvám, který formálně stanovuje požadavky v oblastech ochrany integrity zařízení, správy přístupových práv, řízení aktualizací a hlášení incidentů. Dokument je postaven na principech „least privilege“ a „zero trust“ a určuje, že servisní technik má přístup pouze v rozsahu nezbytném pro konkrétní zásah, a to výhradně za přítomnosti autorizovaného zástupce provozovatele.

Navržená opatření byla konzultována s právním a smluvním oddělením a připravena k implementaci v rámci následujícího servisního cyklu. Přijaté kroky přispívají ke zvýšení právní i provozní jistoty při správě kritické infrastruktury, ke snížení provozních rizik a k posílení bezpečnostní kultury ve spolupráci s externími partnery v souladu s požadavky normy PCI DSS 4.0.

6.2.3. Přehodnocení přístupových práv a kontrola identity servisních techniků

V návaznosti na aktualizaci pravidel pro správu vztahů se servisními partnery došlo k přehodnocení přístupových práv udělených externím technikům provádějícím servisní zásahy na platebních terminálech a souvisejících zařízeních. Tito pracovníci přicházejí do přímého kontaktu s prvky infrastruktury spadajícími do prostředí CDE (Cardholder Data Environment), a proto je nezbytné jejich přístup řídit, evidovat a kontrolovat v souladu s požadavky normy PCI DSS 4.0. Analýza stávajícího stavu ukázala, že přístupy byly doposud řízeny převážně na základě důvěry
a dosavadní spolupráce se servisními partnery. Identifikace techniků často probíhala neformálně, bez jednotného systému pro ověření totožnosti. Zásahy byly mnohdy prováděny bez centrální evidence a v některých případech bez přítomnosti oprávněného zástupce společnosti. Tento přístup představoval riziko z hlediska sledovatelnosti, auditovatelnosti i celkové bezpečnosti.

Na základě zjištěných nedostatků byla navržena opatření směřující ke zvýšení kontroly a transparentnosti. Klíčovým prvkem je zavedení personifikovaných technických identit – každý technik je předem identifikován unikátním ID, které je spojeno s konkrétními zásahy. Přístup k zařízení je umožněn až po ověření totožnosti, například prostřednictvím QR kódu nebo autentizační aplikace, která zároveň eviduje přítomnost technika a přiřazuje ji ke konkrétnímu servisnímu úkonu. Po celou dobu zásahu je přítomen zástupce společnosti, který dohlíží na průběh činnosti a následně potvrzuje, že byla provedena v souladu s interními pravidly. Veškeré servisní činnosti jsou logovány v centrální databázi – systém automaticky zaznamenává datum, čas, jméno technika i zodpovědné osoby z řad interních zaměstnanců. Tyto záznamy jsou následně pravidelně kontrolovány s cílem identifikovat případné nesrovnalosti, jako je neoprávněný přístup, odchylky od schváleného harmonogramu či nesoulad mezi ohlášeným a skutečně přítomným pracovníkem. Tímto způsobem bylo dosaženo výrazného posílení kontroly nad pohybem externích pracovníků a zajištěna plná dohledatelnost všech servisních činností. Navržený systém je v souladu s principy minimálního nezbytného přístupu, odpovědnosti za přístup a zpětné auditní dohledatelnosti, které tvoří základní pilíře řízení přístupů v rámci PCI DSS 4.0. Celkově tak navržená opatření významně přispěla k posílení bezpečnostní kultury při spolupráci s externími partnery a k eliminaci rizik spojených s neoprávněnými nebo nezdokumentovanými zásahy do kritických systémů.

6.3. Zvýšení efektivity interních auditů

Interní audity představují důležitý nástroj pro zajištění kontinuálního souladu s požadavky standardu PCI DSS a pro včasnou detekci nedostatků v provozních a bezpečnostních procesech.

V rámci přechodu na verzi 4.0 této normy bylo nezbytné přehodnotit stávající auditní mechanismy, které byly do značné míry formální, málo hluboké a postrádaly schopnost systematicky vyhodnocovat reálnou připravenost organizace na incidenty nebo nesoulad. Původní praxe v oblasti auditů spočívala především v každodenní kontrole platebních terminálů, prováděné zaměstnanci na prodejnách. Tyto kontroly se soustředily zejména na ověření fyzického stavu zařízení a přítomnosti plomb. Výsledky byly zaznamenávány ručně do lokálního systému nebo hlášeny neformálně, přičemž chyběla centrální koordinace, auditní dohled a především metodika, která by zajistila jednotnost a srovnatelnost mezi jednotlivými pobočkami. V praxi tak vznikal falešný dojem vysoké míry kontroly, ačkoliv v reálném provozu nebyly odhalovány zásadní nedostatky. Na základě výše uvedených skutečností byl navržen a implementován víceúrovňový model interních auditů, založený na kombinaci denních, měsíčních a tematicky zaměřených kontrol. Veškeré aktivity jsou plánovány, sledovány a vyhodnocovány prostřednictvím centralizovaného service portálu. V rámci této digitální platformy byla vytvořena sada kontrolních aktivit, které reflektují jak požadavky příslušné normy, tak specifika maloobchodního prostředí.

První sada nově definovaných auditních aktivit je zaměřena na pravidelnou kontrolu serverové infrastruktury a probíhá s frekvencí jednou ročně. Audit se soustředí na klíčové komponenty datových center, jako jsou servery pro zpracování transakčních údajů, zálohovací systémy, přístupové brány a prvky zajišťující logování a monitoring. V rámci service portálu byl vytvořen samostatný typ auditní aktivity, ve které administrátor vyplňuje kontrolní protokol s více než 40 kontrolními body. Ty se týkají například aktuálnosti firmware, nasazení bezpečnostních záplat, integrity logovacích systémů, stavu šifrovacích klíčů a nastavení přístupových oprávnění na úrovni operačního systému i aplikací.

Druhá vrstva auditních aktivit je tvořena měsíčními kontrolami, které provádí lokální odpovědná osoba. Tento typ auditu má širší záběr a zahrnuje mimo jiné ověřování dodržování přístupových pravidel, aktualizací provozních manuálů, reakčních dob na incidenty a správnosti eskalačních postupů. V service portálu byla integrována šablona auditního formuláře, jenž je po každém měsíčním kole vyplněn a následně předložen ke schválení bezpečnostnímu oddělení. Výsledky se dále agregují do přehledných dashboardů sloužících k vyhodnocování trendů a plánování nápravných opatření.

Třetí sada aktivit se vztahuje k centrálně řízeným tematickým auditům, které se zaměřují na konkrétní rizikové oblasti – například reakce na incidenty mimo běžnou pracovní dobu, správnost přidělování uživatelských práv či zabezpečení vzdáleného přístupu. Tyto audity nejsou předem oznamovány a jejich cílem je objektivní ověření připravenosti personálu reagovat

v souladu s nastavenými postupy. V rámci portálu byly připraveny kontrolní scénáře včetně prostoru pro dokumentaci reakcí, přiložení důkazních materiálů (např. logy, fotografie terminálů) a automatického vyhodnocení souladu s požadavky. Součástí celkového konceptu je také mechanismus zpětné vazby a reakčních cyklů. Každý auditní záznam v portálu umožňuje přidávání komentářů a eskalaci v případě opakujících se nedostatků. V rámci bezpečnostního týmu probíhají pravidelné měsíční porady, na kterých se vyhodnocují výsledky všech auditních aktivit za uplynulé období a navrhují se cílená opatření k nápravě. Tato opatření jsou následně implementována v provozu, což umožňuje flexibilní přizpůsobení interních procesů aktuálním potřebám a snižování provozních rizik.

Nový model interních auditů přináší důraz na důslednost a relevantnost kontrol, a zároveň zajišťuje jednotnost, dohledatelnost a důkazní sílu všech zjištění. Transparentní, datově řízený přístup umožňuje rychlou reakci na zjištěné nedostatky, zvyšuje odolnost vůči lidským selháním a zjednodušuje přípravu na externí audity, certifikace nebo forenzní šetření v případě incidentů. Celková struktura odpovídá požadavkům normy PCI DSS 4.0 a zároveň reflektuje potřebu provozní efektivity v prostředí s rozsáhlou infrastrukturou a mnoha pobočkami.

6.4. Problémy a komplikace při implementaci optimalizovaných procesů

V rámci mezinárodního projektu, jehož cílem bylo implementovat systém pro kontrolu platebních terminálů a jejich instalačních plomby, byla dodána aplikace navržená ke zjednodušení kontrolního procesu oproti dřívější metodě využívající handheld zařízení. Cílem navrhovaného řešení bylo umožnit snadnější ověření stavu plomby, čímž by se eliminovala nutnost manuální kontroly a následného zadávání výsledků do back office.

Implementace této aplikace se však setkala s několika zásadními problémy, které vyplývaly zejména z organizačních nedostatků na straně mezinárodního týmu. Klíčovým problémem byla nedostatečná lokalizace softwarového řešení – aplikace nebyla adekvátně přizpůsobena specifickým podmínkám a provozním požadavkům jednotlivých zemí. Navíc probíhala spolupráce s lokálními partnery velmi pomalu, což výrazně komplikovalo integraci a adaptaci nového systému do stávající infrastruktury. Dalším zásadním nedostatkem byla absence včasného provedení podrobné analýzy rizik, která by umožnila stanovit optimální frekvenci kontrol terminálů a definovat provozní parametry automatizovaného ověřování stavu plomby. Zatížení mezinárodního týmu jinými projekty vedlo k opožděnému rozhodnutí o implementaci, čímž nebyly stanoveny potřebné podmínky pro úspěšné nasazení daného řešení.

V důsledku těchto komplikací se mezinárodní tým rozhodl zrušit povinnou implementaci tohoto systému na globální úrovni a ponechat rozhodnutí o jeho využití na úrovni jednotlivých zemí. Každá země tak musí provést vlastní hodnocení rizik a určit, zda a jakým způsobem může dané řešení odpovídat jejím specifickým provozním potřebám. Absence včasné analýzy rizik vedla k tomu, že frekvence kontrol terminálů nebyla adekvátně stanovena a implementace systému byla odložena na pozdější období. Tato zkušenost poukazuje na nezbytnost důkladného plánování, včasné analýzy rizik a efektivní koordinace mezi mezinárodním a lokálním managementem při zavádění nových technologických řešení. Přestože samotná aplikace nebyla implementována, rozhodnutí o jejím odložení neovlivnilo úroveň zabezpečení terminálů, neboť každá země má nyní možnost samostatně vyhodnotit vhodnost a proveditelnost tohoto řešení vzhledem ke svým specifickým podmínkám.

7. PRŮBĚH AUDITU A JEHO VYSLEDKY

7.1. Provádění auditu

7.1.1. Fáze kancelářské kontroly

V rámci kancelářské fáze auditu se externí auditorská společnost nejprve zaměřila na detailní seznámení se všemi dostupnými podklady a IT infrastrukturou organizace. Auditor pečlivě prostudoval interní směrnice, podrobné provozní postupy, protokoly absolvovaných školení a výsledky předchozí gap analýzy, která reflektovala dosavadní implementaci standardu PCI DSS. Tyto dokumenty poskytly komplexní přehled o tom, jak organizace strukturovala své interní politiky a zda byly postupy řádně implementovány do praxe, s ohledem na aktuální mezinárodní bezpečnostní normy.

Následně auditor provedl rozsáhlou technickou kontrolu serverových systémů a celé síťové infrastruktury. Byl kladen důraz na ověření správnosti konfigurací jednotlivých serverů, funkčnosti logovacích mechanismů a schopnosti systémů adekvátně zaznamenávat bezpečnostní události. Součástí této kontroly bylo také posouzení efektivity segmentace sítě, která je nezbytná pro oddělení citlivých dat od ostatních částí infrastruktury, a ověření správné implementace šifrovacích technologií, jež chrání přenášená i uložená data. Auditor rovněž prověřil správu přístupu a kontrolu oprávnění, aby bylo zajištěno, že pouze oprávněné osoby mají přístup k citlivým informacím, čímž se minimalizuje riziko neoprávněného přístupu či úniku dat.

Na základě získaných informací auditor systematicky shromáždil a strukturoval veškerá data do detailních kontrolních seznamů a metodických pokynů. Tyto nástroje sloužily jako podklad pro další terénní kontroly a umožnily přesně identifikovat oblasti, kde jsou dodržovány stanovené interní postupy, a zároveň odhalit případné nedostatky. Systematizace dat rovněž zahrnovala vyhodnocení souladu s požadavky PCI DSS a identifikaci potenciálních slabých míst, která vyžadují nápravná opatření.

Celkově tato kancelářská fáze auditu představovala strategický krok, který umožnil hluboké porozumění interním procesům a technologickému zázemí organizace. Získané poznatky položily pevný základ pro následné etapy ověřování praktické aplikace optimalizovaných procesů v terénu a umožnily auditorské společnosti objektivně zhodnotit, do jaké míry jsou implementovány a dodržovány optimalizované postupy, což je klíčové pro dosažení plné shody s normami PCI DSS.

7.1.2. Fáze terénní kontroly

V rámci terénní kontroly auditor navštívil náhodně vybrané obchody, aby ověřil, zda jsou zavedené optimalizované procesy a interní směrnice aplikovány v praxi. Auditor se setkal s pracovníky na pokladně, provedl praktické testy a kladl řadu konkrétních otázek zaměřených na ověření jejich znalostí a schopností řešit případné bezpečnostní incidenty. Níže je uveden seznam otázek, které auditor položil, a které plně reflektovaly obsah školení a interních postupů:

- **Jak postupujete v případě výpadku platebního terminálu?**

Zaměstnanci měli vysvětlit, jaké kroky okamžitě podniknout, včetně kontaktování odpovědné osoby a zaznamenání incidentu.

- **Kdo je odpovědný za kontrolu a pravidelnou údržbu terminálu?**

Odpověď měla obsahovat informace o stanovených rolích dle interního RACI modelu.

- **Jak ověřujete, že terminál správně maskuje údaje o platební kartě (zobrazuje pouze poslední čtyři číslice)?**

Zaměstnanci měli potvrdit, že používají stanovené metody kontroly a že jsou obeznámeni s technickými mechanismy šifrování a maskování.

- **Co dělat v případě, že zaznamenáte podezřelou aktivitu či chybu v logování transakcí?**

Odpověď měla obsahovat postup hlášení incidentu, včetně specifikace kontaktů na interní bezpečnostní oddělení.

- **Jaká bezpečnostní opatření máte implementována během zpracování platebních transakcí?**

Zaměstnanci měli uvést jak technická opatření (šifrování, segmentace sítě, logování), tak i organizační postupy (školení, pravidelné kontroly).

- **Jak probíhá vaše pravidelná účast na školeních a aktualizacích interních postupů?**

Odpověď měla potvrdit, že školení byla absolvována a že jsou pravidelně připomínány aktuální bezpečnostní postupy. Po kladení těchto otázek auditor zjistil, že všichni zaměstnanci byli schopni na všechny otázky odpovědět přesně a s potřebnou odbornou terminologií. To dokládalo, že předchozí školení byla efektivní a že optimalizované procesy jsou v praxi uplatňovány, v souladu s interními směrnicemi a normami PCI DSS.

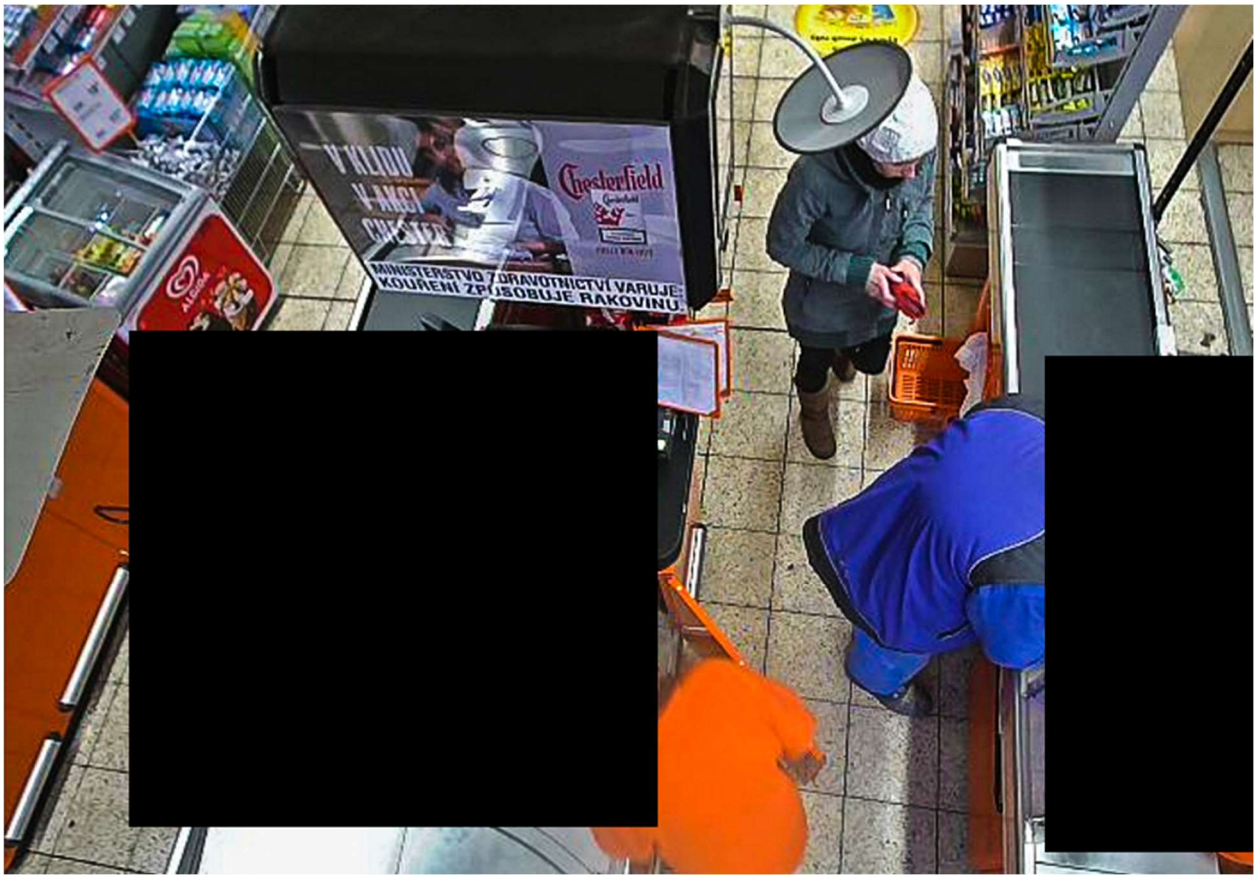
Kromě rozhovorů proběhly i praktické testy, při nichž auditor provedl několik testovacích nákupů. Tyto nákupy měly za cíl ověřit, že platební terminály zobrazují pouze poslední čtyři číslice platebních karet a že jsou implementovány správné šifrovací a maskovací technologie. Auditor také zkontroloval fyzickou bezpečnost zařízení, ověřil správné umístění a funkčnost bezpečnostních kamer, čímž se potvrdila účinnost fyzických ochranných opatření.


Corny Big banán 25,80 B
2 ks x 12,90 Kč/ks
Sleva fronta -3,42
Cena po slevě 22,38
EMCO Super sušenky 25,80 B
2 ks x 12,90 Kč/ks
Sleva fronta -3,42
Cena po slevě 22,38
Popcorn slaný 24,90 B
Sleva fronta -3,30
Cena po slevě 21,60
Adventní kalendář 19,80 B
2 ks x 9,90 Kč/ks
Sleva fronta -2,60
Cena po slevě 17,20
K PLATBĚ 327,73
Karta 327,73
Celková zaplacená částka 327,73
18/12/23 09:49 Účtenka číslo 00292
Terminál: [redacted]
PRODEJ 327.73 CZK
**** **** **** 4543 / 01 (L) VISA
A0 00 00 00 03 10 10 Visa Debit
Visa Contactless
SEQ ID: 002:698:065, Autoriz. kód 755727
No Pin *NO REFUND*
Celková sleva 50,00
B 15% DPH z 327,73 42,75

Obrázek 11 Příklad údajů o kartě na účtence

Zdroj: vlastní

Další zásadní kontrolou byla revize fyzických bezpečnostních opatření u platebních terminálů. Auditor ověřil, zda je u terminálů instalován ochranný maskovací prvek ve formě černého čtverce, který zajišťuje, že displej terminálu, včetně zadávacího pole pro PIN, není z vnější strany viditelný. Tímto opatřením se minimalizuje riziko neoprávněného sledování citlivých údajů zákazníků. Auditor zhodnotil, že ochranná maska byla správně umístěna a funkčně plní svůj účel, čímž přispívá k celkové fyzické bezpečnosti platebních terminálů.



Obrázek 12 Příklad záznamu z videokamery

Zdroj: [30]

Tímto opatřením se minimalizuje riziko neoprávněného sledování citlivých údajů zákazníků. Auditor zhodnotil, že ochranná maska byla správně umístěna a funkčně plní svůj účel, čímž přispívá k celkové fyzické bezpečnosti platebních terminálů.

Tento komplexní přístup k terénní kontrole umožnil auditorské společnosti získat detailní a objektivní pohled na praktickou aplikaci zavedených optimalizovaných procesů. Na základě získaných informací auditor formálně potvrdil, že zaměstnanci odpověděli na všechny položené otázky v souladu s očekávanými standardy, a že technické i organizační postupy jsou implementovány tak, jak bylo plánováno.

7.2. Výsledky auditu verze 4 PCI DSS

Výsledky auditu verze 4 PCI DSS potvrdily, že organizace dosáhla plné shody s požadavky standardu bez identifikace jakýchkoli závažných nebo vysokorizikových nedostatků. Externí auditor ocenil důslednou implementaci technických opatření – zejména segmentaci Cardholder Data Environment, komplexní šifrování dat v klidu i v přenosu a efektivní správu přístupových práv, které byly integrovány do stávající IT infrastruktury bez kompromisů na bezpečnosti.

Rovněž bylo potvrzeno, že interní procesy pro periodické kontroly terminálů, správu patchů, auditní logování a eskalaci bezpečnostních incidentů jsou jednoznačně definovány, dokumentovány a v praxi konzistentně uplatňovány všemi zúčastněnými pracovníky. Mezi konkrétní zlepšení, která audit potvrdil, patřilo zejména:

- **Standardizace interních kontrolních procesů:** Zavedení jednotných metodik a pravidelných auditů umožnilo rychlejší identifikaci a nápravu případných odchylek, což významně zvýšilo efektivitu řízení bezpečnostních incidentů.
- **Optimalizace školení zaměstnanců:** Aktualizovaná a zjednodušená školení přispěla k lepší připravenosti pracovníků reagovat na bezpečnostní situace, což vedlo ke zvýšení úrovně provozní bezpečnosti.
- **Zvýšení transparentnosti monitoringu:** Nasazení moderních nástrojů pro centralizovanou správu a sledování bezpečnostních událostí umožnilo přesnější evidenci provozních dat a zlepšilo komunikaci mezi jednotlivými odděleními.

Praktické testy a simulace kybernetických incidentů prokázaly bezchybnou funkčnost klíčových bezpečnostních mechanismů, včetně konfigurace firewallů, IDS/IPS systémů a monitoringových nástrojů. Auditor rovněž zdůraznil vysokou úroveň znalostí personálu, který během strukturovaných rozhovorů a testovacích scénářů ukázal důkladné pochopení postupů pro řešení případných anomálií či poruch terminálů. Veškerá zjištění byla shledána jako neklíčová — týkala se pouze drobných úprav dokumentace a zpřesnění některých interních směrnic, což neovlivnilo celkové hodnocení souladu se standardem.

Na základě těchto výsledků společnost X úspěšně obdržela oficiální PCI DSS certifikaci verze 4. Tento úspěch potvrzuje, že implementovaná opatření nejen splňují přísné mezinárodní požadavky, ale také významně posilují bezpečnostní kulturu a provozní odolnost organizace vůči aktuálním i budoucím kybernetickým hrozbám.

ZÁVĚR

Diplomová práce se zaměřila na komplexní problematiku implementace nové verze standardu PCI DSS v prostředí rozsáhlé maloobchodní sítě. Cílem práce bylo nejen analyzovat aktuální stav zabezpečení citlivých platebních údajů a identifikovat klíčová slabá místa v procesech organizace, ale především navrhnout a ověřit optimalizační opatření, která povedou k dosažení plné shody se standardem PCI DSS verze 4 a ke zvýšení úrovně bezpečnosti v každodenním provozu.

Provedená analýza prokázala, že ačkoli má sledovaná organizace zavedené základní bezpečnostní politiky a technologickou infrastrukturu na vysoké úrovni, v řadě případů došlo k formálnímu plnění požadavků bez hlubší reflexe aktuálních hrozeb a reálné efektivity procesů. Identifikována byla například neaktuální dokumentace, nejasnosti v přidělení odpovědností dle RACI modelu nebo nízká frekvence praktických auditních kontrol.

Na základě gap analýzy byla navržena konkrétní opatření, mezi nimiž klíčovou roli sehrály modernizace auditních mechanismů, implementace formálního RACI rámce a zlepšení spolupráce se servisními partnery. Všechna tato opatření byla navržena s důrazem na provozní realizovatelnost, udržitelnost v rámci každodenního provozu a podporu bezpečnostní kultury.

Praktická fáze práce, která zahrnovala jak interní validaci opatření, tak závěrečný audit externím subjektem, prokázala, že navržené změny vedly k dosažení plné shody s požadavky PCI DSS 4 bez zjištění kritických nedostatků. Kromě technických zlepšení byla potvrzena i vysoká úroveň připravenosti zaměstnanců a schopnost organizace rychle reagovat na potenciální incidenty.

Výsledky této práce ukazují, že úspěšná implementace standardu PCI DSS není pouze otázkou technického nastavení, ale vyžaduje systematický přístup k optimalizaci procesů, průběžné vzdělávání zaměstnanců, funkční interní komunikaci a důsledné řízení bezpečnostních rizik. Práce rovněž potvrdila význam iterativního přístupu a potřebu pravidelného přehodnocování nastavených opatření s ohledem na vývoj kybernetických hrozeb. Tato zjištění mohou sloužit jako inspirace i pro další organizace působící v oblasti maloobchodu, které usilují o zvýšení ochrany zákaznických dat a o posílení důvěry veřejnosti v digitální platební systémy.

POUŽITÁ LITERATURA

1. WRIGHT, Steve. *PCI DSS: A Practical Guide to implementing and maintaining compliance.* místo neznámé : IT Governance Publishing, 2011. 9781849281881.

2. What Is PCI Compliance? *Fortinet.* [Online] [Citace: 15. 03 2025.] https://www.fortinet.com/resources/cyberglossary/what-is-pci-compliance.

3. Levašov, Petr. *Cyberfortress: Komplexní průvodce počítačovou bezpečností.* Petrohrad : Piter, 2024 г. 9785446121250.

4. What is Defense in Depth? Best Practices for Layered Security. *WIZ.* [Online] 2024. 11 8. [Citace: 22. 03 2025.] https://www.wiz.io/academy/defense-in-depth.

5. *A guide to PCI compliance.* [Online] Stripe. [Citace: 21. 02 2025.] https://stripe.com/en-cz/guides/pci-compliance.

6. Arthur B. Cooper Jr., Jeff Hall, David Mundhenk, Ben Rothke. *The Definitive Guide to PCI DSS Version 4.* místo neznámé : Apress, 2023. 9781484292877.

7. Herrera, Andrea. 22 Payment Fraud Trends & Statistics You Should Know in 2024. *Fit small business.* [Online] 27. 02 2024. [Citace: 22. 03 2025.] https://fitsmallbusiness.com/payment-fraud-statistics/.

8. Threat Intelligence . Retail Cybersecurity: Threats, Statistics and Best Practices. *Threat Intelligence.* [Online] 06. 12 2024. [Citace: 25. 02 2025.] https://www.threatintelligence.com/blog/retail-cybersecurity.

9. Jason Edwards, Griffin Weaver. *The Cybersecurity Guide to Governance, Risk, and Compliance.* místo neznámé : Wiley, 2024. 9781394250196.

10. eset. Malware. *eset.* [Online] [Citace: 21. 03 2025.] https://www.eset.com/cz/malware/.

11. M., Yaqub. 10+ Retail Cybersecurity Statistics: A Must-Know in 2024. *BusinessDasher.* [Online] 23. 09 2024. [Citace: 22. 03 2025.] https://www.businessdasher.com/retail-cybersecurity-statistics/.

12. Boboev, Sam. Deep Dive: Building a Credit Card Payment Processing Platform and Payment Gateway on AWS. *FW.* [Online] 22. 12 2024. [Citace: 12. 02 2025.] https://www.fintechwrapup.com/p/deep-dive-building-a-credit-card.

13. PCI Security Standards Council. pcisecuritystandards. *PCI Security standarts.* [Online] 06 2018. [Citace: 23. 03 2023.] https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

14. Tripwire. Explaining the PCI DSS Evolution & Transition Phase. *Fortra.* [Online] 26. 02 2023. [Citace: 22. 03 2025.] https://www.tripwire.com/state-of-security/explaining-pci-dss-evolution-transition-phase.

15. COOPER Art, Jeff HALL, David MUNDHENK, Ben ROTHKE. *He Definitive Guide to PCI DSS Version 4.* Berlin : Springer, 2023. 9781484292877.

16. Cymulate. How to Make Your Security Posture PCI DSS v4.0 Compliant. *Cymulate.* [Online] 21. 01 2025. [Citace: 18. 02 2025.] https://cymulate.com/blog/security-posture-pci-dss-v4-0-compliant/.

17. 5 Consequences of PCI Non-Compliance. *iXOpay.* [Online] 01. 07 2024. [Citace: 23. 03 2025.] https://www.ixopay.com/blog/5-consequences-of-pci-noncompliance#:~:text=Fines%20from%20payment%20processors%20can,and%20a%20company%20attains%20compliance..

18. What are the Consequences of Non-Compliance with PCI DSS? *vincworks.* [Online] [Citace: 14. 03 2025.] https://vinciworks.com/blog/what-are-the-consequences-of-non-compliance-with-pci-dss/.

19. ThinkFromSoul. Serverless Architecture of Starbucks. *Medium.* [Online] 25. 12 2023. [Citace: 23. 1 2025.] https://medium.com/@payalswami/serverless-architecture-of-starbucks-468b921c9de9.

20. Williams, Branden a Adamson, James. How Starbucks is Revolutionizing Mobile (micro) Payments. *brandenwilliams.* [Online] 24. 1 2013. [Citace: 29. 1 2025.] https://www.brandenwilliams.com/blog/2013/01/24/how-starbucks-is-revolutionizing-micropayments/.

21. Information Systems at Starbucks. *blogspot.* [Online] 10. 11 2014. [Citace: 25. 1 2025.] https://starbucksinformationsystem.blogspot.com/2014/11/starbucks_10.html.

22. Juvenile. What Is The Procedure To Integrate A Payment Gateway Stripe. *coronatodays.* [Online] 21. 02 2025. [Citace: 22. 02 2025.] https://coronatodays.com/what-is-the-procedure-to-integrate-a-payment-gateway-stripe/.

23. Kirk, Jeremy. Neiman Marcus Says 4.6 Million Affected by Data Breach. *bankinfosecurity.* [Online] 1. 10 2021. [Citace: 21. 2 2025.] https://www.bankinfosecurity.com/neiman-marcus-says-46m-affected-by-data-breach-a-17658.

24. Vijayan, Jaikumar. After Target, Neiman Marcus breaches, does PCI compliance mean anything? *Computer world.* [Online] 21. 1 2014. [Citace: 16. 02 2025.] https://www.computerworld.com/article/1510394/after-target-neiman-marcus-breaches-does-pci-compliance-mean-anything.html.

25. Kosseff, Jeff. *Cybersecurity Law.* místo neznámé : Wiley, 2022. 9781119822172.

26. E.Ekimov. Požadavky na informační bezpečnost pro účastníky trhu transakční infrastruktury. *CyberLeninka.* [Online] 2018. [Citace: 19. 03 2025.] https://cyberleninka.ru/article/n/trebovaniya-k-informatsionnoy-bezopasnosti-dlya-uchastnikov-rynka-tranzaktsionnoy-infrastruktury.

27. R. Faizulin, M. Demichev, A. Ogol, A. Bondarev. The role of PCI DSS in Informazion Security. *cyberleninka.* [Online] [Citace: 20. 03 2025.] https://cyberleninka.ru/article/n/rol-pci-dss-v-obespechenii-informatsionnoy-bezopasnosti.

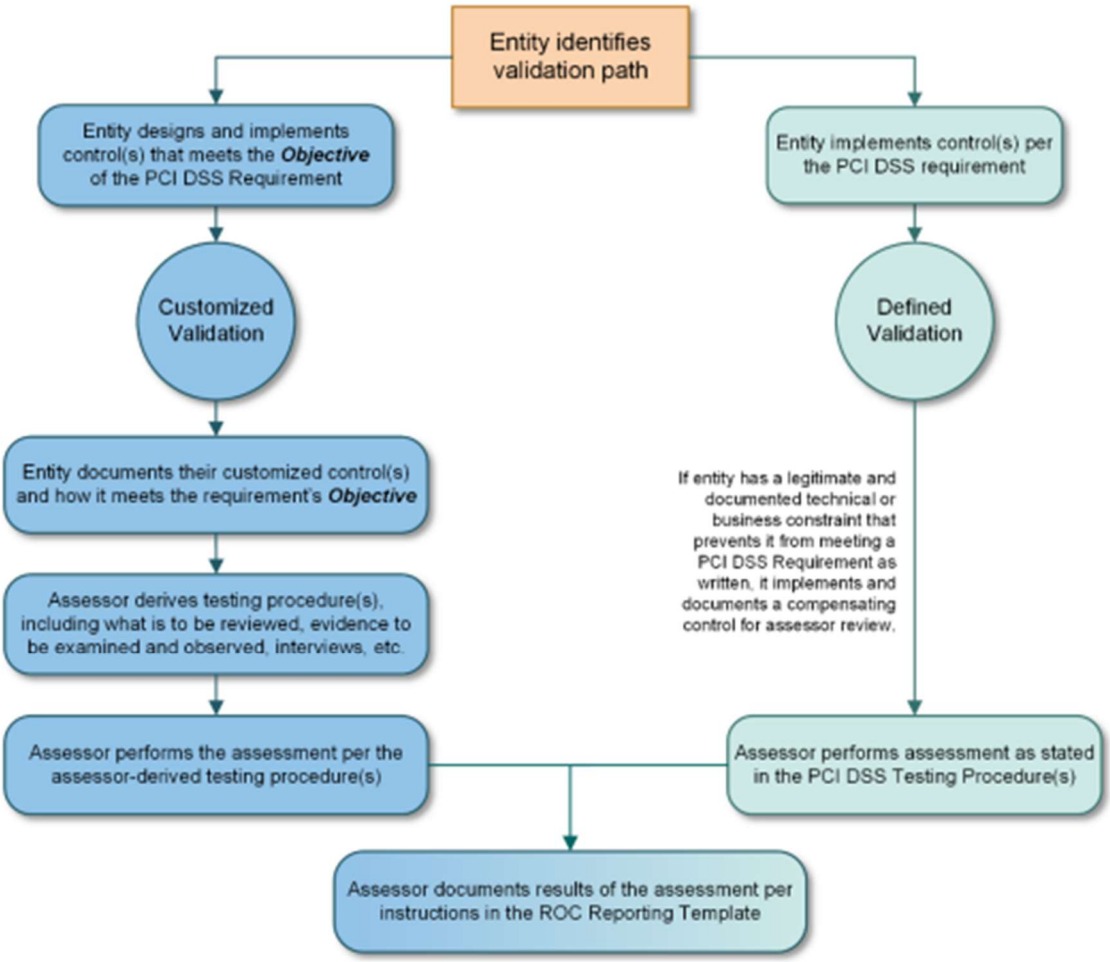
28. Rane, Satya. What are the 12 requirements of PCI DSS Compliance? *ControlCase.* [Online] [Citace: 21. 03 2025.] https://www.controlcase.com/what-are-the-12-requirements-of-pci-dss-compliance/.

29. Talmi, Yarom. How to Train Employees for PCI Compliance. *Cybeready.* [Online] 31. 03 2022. [Citace: 23. 03 2025.] https://cybeready.com/awareness-training/how-to-train-employees-for-pci-compliance.

30. Ondráček, Vojtěch. Nesledují i vás? Přenosy z bezpečnostních kamer jsou volně dostupné na internetu. *ISCAL.* [Online] 2016. 01 09. [Citace: 20. 03 2025.] https://zpravy.tiscali.cz/nesleduji-i-vas-prenosy-z-bezpecnostnich-kamer-jsou-volne-dostupne-na-internetu-270745.

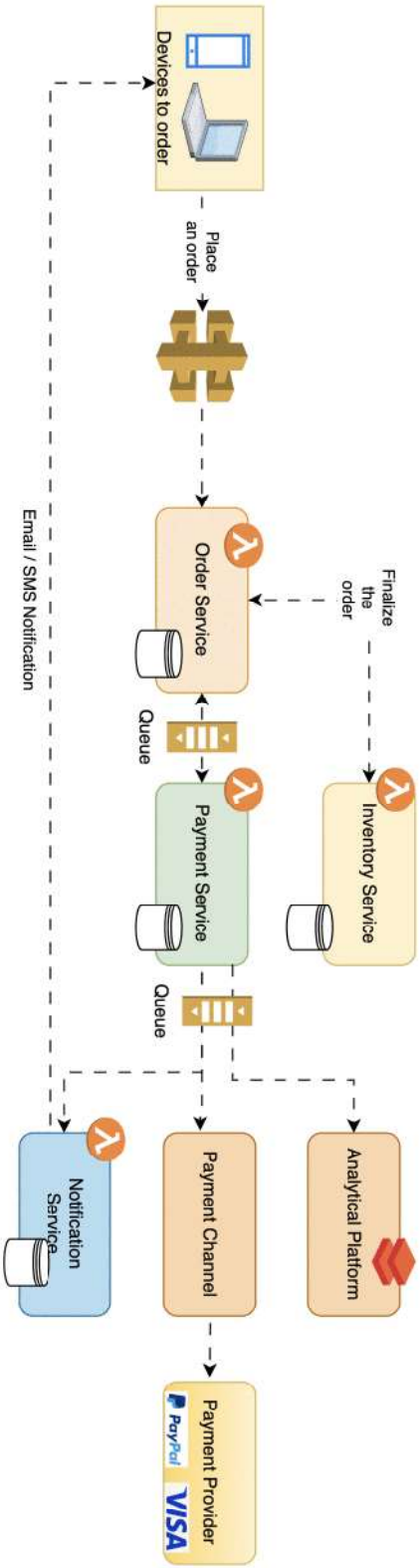
PŘÍLOHY

Příloha 1 Schéma iterativního cyklu od mapování procesů po validaci nových opatření v prostředí PCI DSS



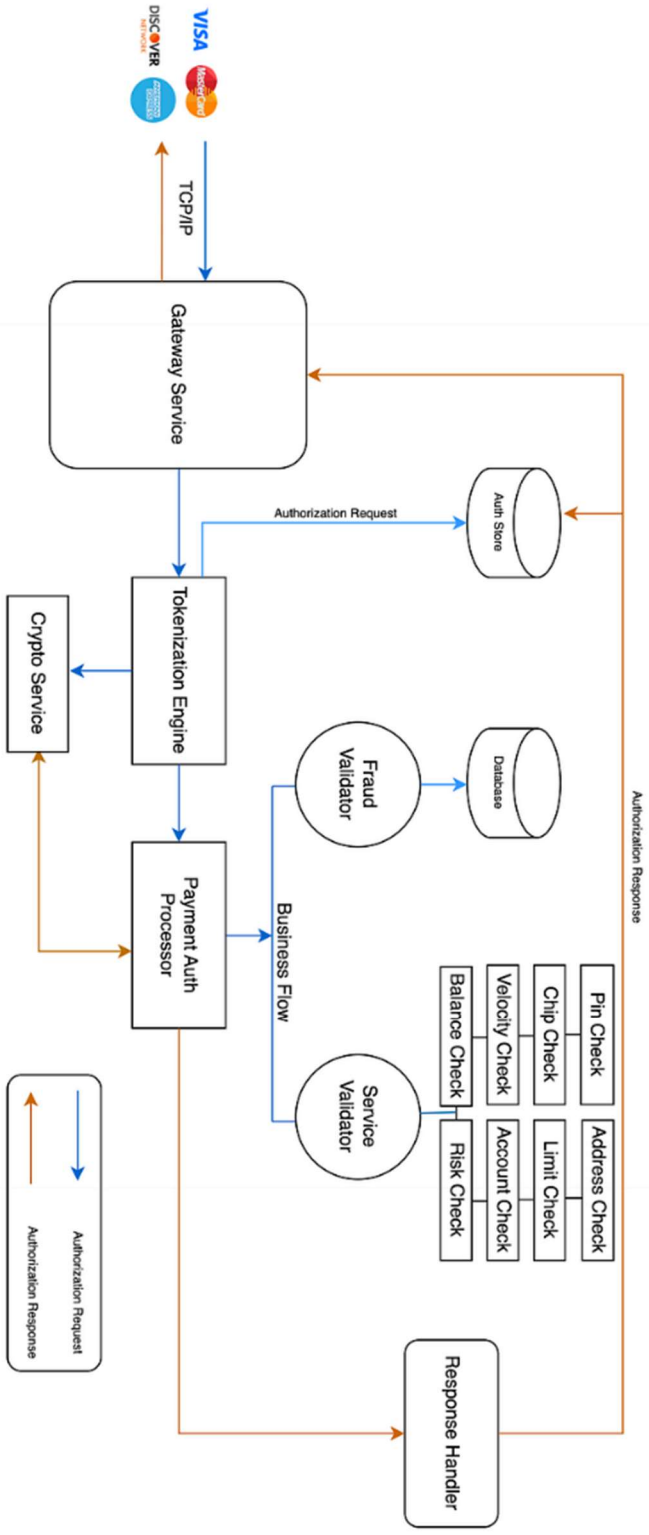
Zdroj **[16]**

Příloha 2 Schéma toku dat mezi mobilní aplikací, platební bránou a backendovými systémy Starbucks



Zdroj **[19]**

Příloha 3 Ilustrační procesní schéma zachycující cestu karetních dat od pokladní zóny až po centrální server



Zdroj [12]

Příloha 4 Příklad kontrolní aktivity

Zdroj: vlastní

Příloha 5 Ukázka RACI tabulky

PCI DSS Requirements	Status	ROLES										
		IT					External					
		IT Network Team	CIO	IT Service & Support	IT BC Store & Customer Systems	ISO	Operationa l/ Verwaltun g	SIT Network	HR	Field service	ČSOB
Requirement 1 - Install and Maintain Network Security Controls											
1.2.3 Accurate Network Diagram is maintained		R				A		C			
1.2.5 Documentation of all services, ports and protocols used in PCI and their business justification.						A		I			R
1.3.1 Inbound traffic to the CDE is restricted as follows: () To only traffic that is necessary. () All other traffic is specifically denied.						A					R
1.3.2 Outbound traffic from the CDE is restricted as follows: () To only traffic that is necessary. () All other traffic is specifically denied.						A					R
1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.						A					R
Requirement 2 - Apply Secure Configurations to All System Components.											
2.2.2 Vendor default accounts are managed as follows: () If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. () If the vendor default account(s) will not be used, the account is removed or disabled.		R		R	R	A					R
2.2.7 All non-console administrative access is encrypted using strong cryptography.		R		R	R	A					R
Requirement 3 - Protect Stored Account Data											
3.1.1 All security policies and operational procedures that are identified in Requirement 3 are: () Documented. () Kept up to date. () In use. () Known to all affected parties.		I	A	I	I	R	I		I	I	
3.3.1 SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.						A	R				R
3.3.1.1 The full contents of any track are not retained upon completion of the authorization process.						A					R
3.3.1.2 The card verification code is not retained upon completion of the authorization process.						A	R				
3.3.1.3 The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.						A	R				R
3.4.1 PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.						A	R				R

Zdroj: vlastní

Příloha 6 Ukázka gap analysis tabulky

PCI DSS TL ID	TL Defined Approach	PCI	Defined Approach Requirements	Defined Approach Testing Procedures	Guidance	Laymen Terms	Evidence	Interview	Documentation	Status
1.1	1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.	1.1.2	1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood. [CUSTOMIZED APPROACH OBJECTIVE]: Day-to-day responsibilities for performing all the activities in Requirement 1 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	1.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 1 are documented and assigned. 1.1.2.b Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and are understood.	Purpose: If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur. Good Practice: Roles and responsibilities may be documented within policies and procedures or maintained within separate documents. As part of communicating roles and responsibilities, entities can consider having personnel acknowledge their acceptance and understanding of their assigned roles and responsibilities. Examples: A method to document roles and responsibilities is a responsibility assignment matrix that includes who is responsible, accountable, consulted, and informed (also called a RACI matrix).	Definovaná odpovědnost za jednotlivé úkoly při řízení síťových prvků (v návaznosti na platební terminály). Kdo řídí tyhle procesy, kdo je vykonává, kdo je schvaluje atd.	RACI Matrix - Neexistuje	TBD	RACI Matrix - Neexistuje	Not OK
1.2	1.2 Network security controls (NSCs) are configured and maintained.	1.2.3	1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks. [CUSTOMIZED APPROACH OBJECTIVE]: A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available. [APPLICABILITY NOTES]: A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement.	1.2.3.a Examine diagram(s) and network configurations to verify that an accurate network diagram(s) exists in accordance with all elements specified in this requirement. 1.2.3.b Examine documentation and interview responsible personnel to verify that the network diagram(s) is accurate and updated when there are changes to the environment.	Purpose: Maintaining an accurate and up-to-date network diagram(s) prevents network connections and devices from being overlooked and unknowingly left unsecured and vulnerable to compromise. A properly maintained network diagram(s) helps an organization verify its PCI DSS scope by identifying systems connecting to and from the CDE. Good Practice: All connections to and from the CDE should be identified, including systems providing security, management, or maintenance services to CDE system components. Entities should consider including the following in their network diagrams: () All locations, including retail locations, data centers, corporate locations, cloud providers, etc. () Clear labeling of all network segments. () All security controls providing segmentation, including unique identifiers for each control (for example, name of control, make, model, and version). () All in-scope system components, including NSCs, web application firewalls, anti-malware solutions, change management solutions, IDS/IPS, log aggregation systems, payment terminals, payment applications, HSMs, etc. () Clear labeling of any out-of-scope areas on the diagram via a shaded box or other mechanism. () Date of last update, and names of people that made and approved the updates. () A legend or key to explain the diagram. Diagrams should be updated by authorized personnel to ensure diagrams continue to provide an accurate description of the network.	Síťové schéma/diagram ukazující aktuální připojení platebních terminálů, hlavně všechny spoje k a od platebního terminálu (případně jeho VLAN)	Diagram - Není	N/A		Not OK
1.2	1.2 Network security controls (NSCs) are configured and maintained.	1.2.5	1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need. [CUSTOMIZED APPROACH OBJECTIVE]: Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.	1.2.5.a Examine documentation to verify that a list exists of all allowed services, protocols, and ports, including business justification and approval for each. 1.2.5.b Examine configuration settings for NSCs to verify that only approved services, protocols, and ports are in use.	Purpose: Compromises often happen due to unused or insecure services, protocols, and ports that are enabled but not in use are often overlooked and left unsecured and unpatched. By identifying the services, protocols, and ports necessary for business, entities can ensure that all other services, protocols, and ports are disabled or removed. Good Practice: The security risk associated with each service, protocol, and port allowed should be understood. Approvals should be granted by personnel independent of those managing the configuration. Approving personnel should possess knowledge and accountability appropriate for making approval decisions.	Bude potřeba dokumentace všech povolených služeb, protokolů a portů pro ště kde se nacházejí platební terminály.	Dokumentace sítových nastavení - Není			Not OK
1.2	1.2 Network security controls (NSCs) are configured and maintained.	1.2.6	1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated. [CUSTOMIZED APPROACH OBJECTIVE]: The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.	1.2.6.a Examine documentation that identifies all insecure services, protocols, and ports in use to verify that for each, security features are defined to mitigate the risk. 1.2.6.b Examine configuration settings for NSCs to verify that the defined security features are implemented for each identified insecure service, protocol, and port.	Purpose: Compromises take advantage of insecure network configurations. Good Practice(): If insecure services, protocols, or ports are necessary for business, the risk posed by these services, protocols, and ports should be clearly understood and accepted by the organization, the use of the service, protocol, or port should be justified, and the security features that mitigate the risk of using these services, protocols, and ports should be defined and implemented by the entity. [Further Information]: For guidance on services, protocols, or ports considered to be insecure, refer to industry standards and guidance (for example, from NIST, ENISA, OWASP).	V případě použití nezabezpečených služeb, protokolů nebo portů je potřeba definovat a implementovat bezpečnostní opatření.			n/a bude vyžadovat z předchozího seznamu	Partial

Zdroj: vlastní