BEZPEČNOSTNÉ POLITIKY A DOKUMENTÁCIA HACKME BANK

ABSTRACT
Finálna dokumentácia
k projektu v kurze
Informačná bezpečnosť

Marek Hrabčák

Obsah

História dokumentu

Verzia	Popis	Upravil
1.0	Vznik dokumentu	Marek Hrabčák

Úvod

Informácie o organizácii

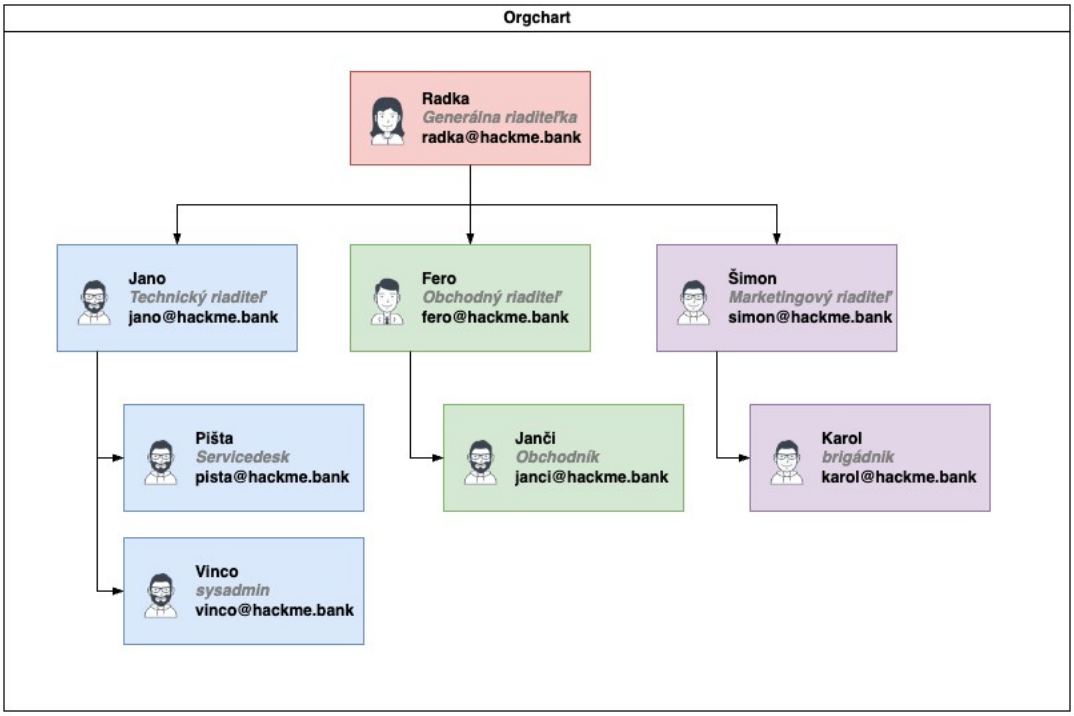
HackMeBank je banková inštitúcia pôsobiaca v celom digitálnom priestore. Nepodlieha regulácii žiadnej centrálnej banky. HackMeBank nemá sídlo podnikania. Všetky služby HackMeBank sú ponúkané v stave v akom sú a bez akej-koľvek záruky.

Ďalšie informácie o banke:

Názov	Popis
Klienti	anonymní klienti, roboti, fyzické a právnické osoby
Licencia	HackMeBank pre svoju činnosť nepotrebuje licenciu
Technické normy	ISO 27001
Produkty	bežné účty, úvery, hypotéky, krypto operácie, anonymné platby

Organizačná štruktúra

HackMeBank má jednoduchú a prehľadnú organizačnú štruktúru. Banka má výkonného riaditeľa, ktorý je zodpovedný za finančné záležitosti, vrátane rozhodnutí o investíciách a obchodných operáciách. Vedenie je podporované viacerými oddeleniami, ako sú oddelenie financií, oddelenie obchodu, oddelenie rizika a oddelenie správy majetku. Každé oddelenie má vedúceho, ktorý je zodpovedný za vedenie a riadenie svojho tímu. Tím je zložený z odborníkov v oblasti financií a rizika, ktorí sú zodpovední za riadenie finančných a rizikových operácií. Každé oddelenie má aj vlastnú podporu, ako je IT, účtovníctvo, právne služby a ďalšie. Banka tiež zamestnáva viacerých externých odborníkov, ako sú audítori a právnici.



Obrázok 1 Organizačná štruktúra

Riadenie rizík

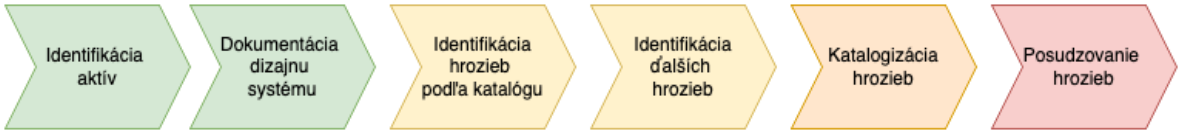
Hrozba je akákoľvek možná udalosť, ktorá môže poškodiť systém alebo dáta.
Zraniteľnosť je miera, v ktorej je systém alebo dáta náchylný na poškodenie spôsobené hrozbou.
Riziko je kombinácia hrozby a zraniteľnosti, ktorá môže mať negatívny vplyv na organizáciu.
HackMeBank vyžaduje, aby boli identifikované všetky možné hrozby, zraniteľnosti a riziká. Prvým krokom je vyhodnotenie hrozieb a zraniteľností. Následne je potrebné stanoviť, aké riziká sú spojené s konkrétnymi hrozbami a zraniteľnosťami. Po určení rizík je potrebné zvoliť adekvátne opatrenia na zmiernenie alebo elimináciu rizík.

(rizík)

Obrázok 2 Postup vyhodnocovania rizík

Identifikácia hrozieb

Hrozba je čokoľvek, čo môže poškodiť informačné aktívum (môže to byť spôsobené človekom alebo prírodnou udalosťou). HackMeBank aplikuje identifikáciu hrozieb pomocou metodiky S.T.R.I.D.E.
S.T.R.I.D.E je model hrozieb, ktorý sa používa na pomoc pri zdôvodňovaní a hľadaní hrozieb pre systém. Používa sa v spojení s modelom cieľového systému, ktorý je možné zostaviť paralelne s existujúcim modelom. Za prípravu cieľového modelu systému je zodpovedný manažér kybernetickej bezpečnosti. Popis procesu identifikácie hrozieb je na nasledujúcom obrázku.



Obrázok 3 Postup vyhodnocovania hrozieb

S.T.R.I.D.E hrozby

Názov	Popis
Spoofing	Podvrhnutie identity používateľa
Tampering	Manipulácia
Repudiation	Odmietnutie
Information disclosure	Zverejnenie informácie
Denial of service	Odmietnutie služby
Elevation of privilege	Povýšenie privilégia

Katalóg hrozieb je technická pomôcka pri identifikácii hrozieb a jeho aktualizáciu zodpovedá manažér kybernetickej bezpečnosti. Každá novo identifikovaná hrozba je pridaná do katalógu hrozieb a slúži ako pomôcka pri ďalšom modelovaní hrozieb.

Katalóg hrozieb

Názov	Popis
Core system	Falšovanie skladieb, manipulácia s dátami klientov, odmietnutie služby
Office 365	Manipulácia s dátami v kľude, zverejnenie informácií
Digitálne kanály	Odmietnutie služby, zverejnenie informácií, manipulácia s dátami

Zraniteľnosti

Zraniteľnosť je slabosť, ktorú možno použiť na poškodenie informačného aktíva. V HackMeBank sú používané nasledujúce zdroje zraniteľnosti:

Názov	Popis
CVE	Verejná databáza známych zraniteľnosti https://www.cvedetails.com/
OpenVas	Aplikácia na skenovanie a identifikovanie známy zraniteľnosti v systémoch HackMeBank

Katalóg zraniteľností je pomôcka pri identifikovaní známych zraniteľností v systémoch HackMeBank.

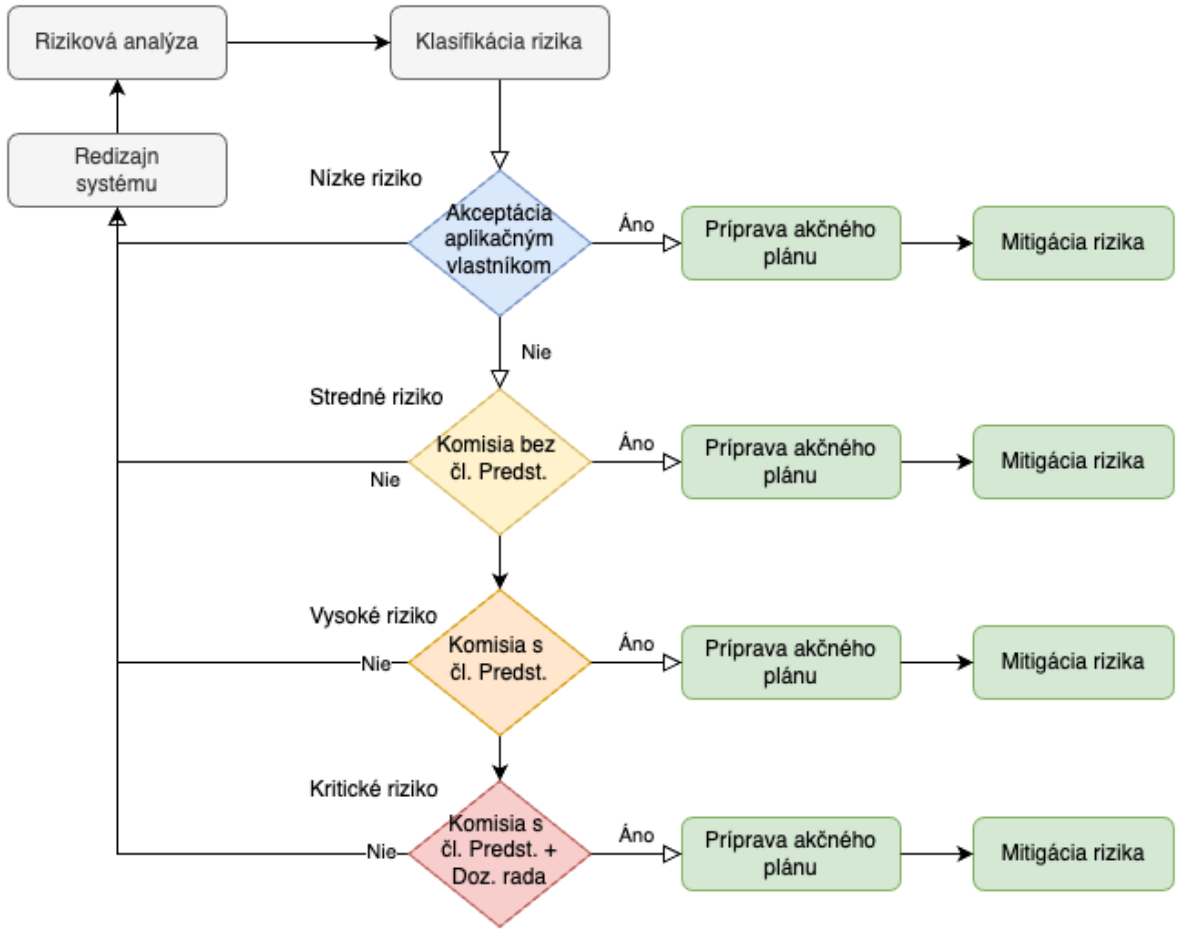
Názov	Skratka	Popis a dopad
Broken Access Control	BAC	Nedostatočná autentizácia
Cryptographic Failures	CF	Zraniteľnosť v šifrovaní
Injection	IJ	Zneužitie chyby v kóde aplikácie
Insecure Design	ID	Zneužitie chyby v dizajne
Security Misconfiguration	SM	Nedostattočná konfigurácia, napr. firewall.
Vulnerable and Outdated Components	VOC	Nedostatočná aktualizácia
Identification and Authentication Failures	IAF	Neodhalené chyby v autentizácii
Software and Data Integrity Failures	SDIF	Nedostatočne otestovaný softvér
0-day vulnerability	0D	Výskyt zraniteľnosti, na ktorú neexistuje záplata
Vendor Lock-in	VL	Závislosť na vendorovi
Loss of device	LoD	Strata zariadenia
Fire	FI	Požiar
Natural disaster	ND	Prírodné živly
Regulatory changes	RCH	Zmeny legislatívy

Zodpovednosť
Za identifikáciu zraniteľností zodpovedá oddelenie bezpečnosti. Popis procesu identifikácie zraniteľností je na nasledujúcom obrázku.

Obrázok 4 Popis procesu identifikácie zraniteľností

Kritériá akceptovania rizika

Popis procesu akceptovania rizika je na nasledujúcom obrázku:



Obrázok 5 Popis procesu akceptovania rizika

Tabuľka s kompetenciami na akceptáciu rizika

Miera rizika	Popis
Nízke	Akceptácia biznis vlastníkom
Stredné	Akceptácia komisiou bez člena predstavenstva
Vysoké	Akceptácia komisiou vrátane člena predstavenstva
Kritické	Akceptácia komisiou + člen Predstavenstva + člen Dozornej rady

Kritéria pravdepodobnosti a dopadu

Kritériá na vykonávanie hodnotenia rizika informačnej bezpečnosti sú určované pomocou pravdepodobnosti a dopadu rizika. V nasledujúcej tabuľke sú uvedené kritéria pre určenie hodnoty pravdepodobnosti a dopadu.

Kritéria pravdepodobnosti

Názov	Popis
Threat Agent Factors	Úroveň zručností - Ako technicky zručná je táto skupina agentov hrozieb? Žiadne technické zručnosti (1), niektoré technické zručnosti (3), pokročilý používateľ počítača (5), sieťové a programovacie zručnosti (6), zručnosti prenikania bezpečnosti (9) Motív - Ako je táto skupina agentov hrozieb motivovaná nájsť a zneužiť túto zraniteľnosť? Nízka alebo žiadna odmena (1), možná odmena (4), vysoká odmena (9) Príležitosť - Aké zdroje a príležitosti sú potrebné na to, aby táto skupina agentov hrozieb našla a zneužila túto zraniteľnosť? Vyžaduje sa úplný prístup alebo drahé zdroje (0), vyžaduje sa špeciálny prístup alebo zdroje (4), vyžaduje sa určitý prístup alebo zdroje (7), nevyžaduje sa žiadny prístup ani zdroje (9) Veľkosť - Aká veľká je táto skupina agentov hrozieb? Vývojári (2), správcovia systému (2), používatelia intranetu (4), partneri (5), overení používatelia (6), anonymní používatelia internetu (9)
Vulnerability Factors	Jednoduchosť objavovania - Aké ľahké je pre túto skupinu agentov hrozieb odhaliť túto zraniteľnosť? Prakticky nemožné (1), ťažké (3), ľahké (7), dostupné automatizované nástroje (9) Jednoduchosť zneužitia - Aké ľahké je pre túto skupinu agentov hrozieb skutočne zneužiť túto zraniteľnosť? Teoretické (1), ťažké (3), ľahké (5), dostupné automatizované nástroje (9) Povedomie - Ako dobre je táto zraniteľnosť voči tejto skupine agentov hrozieb? Neznáme (1), skryté (4), zrejmé (6), verejne známe (9) Detekcia narušenia - Aká je pravdepodobnosť, že zneužitie bude zistené? Aktívna detekcia v aplikácii (1), zaznamenaná a skontrolovaná (3), zaznamenaná bez kontroly (8),

	neprihlásená (9)

Kritéria dopadu

Názov	Popis
Technical Impact Factors	Strata dôvernosti - Koľko údajov by sa mohlo zverejniť a aké citlivé sú? Minimálne zverejnené necitlivé údaje (2), minimálne zverejnené kritické údaje (6), zverejnené rozsiahle necitlivé údaje (6), zverejnené rozsiahle kritické údaje (7), všetky zverejnené údaje (9) Strata integrity - Koľko údajov by mohlo byť poškodených a ako poškodené? Minimálne mierne poškodené údaje (1), minimálne vážne poškodené údaje (3), rozsiahle mierne poškodené údaje (5), rozsiahle vážne poškodené údaje (7), všetky údaje úplne poškodené (9) Strata dostupnosti - Koľko služieb by sa mohlo stratiť a aké dôležité sú? Minimálne prerušenie sekundárnych služieb (1), prerušenie minimálnych primárnych služieb (5), prerušenie rozsiahlych sekundárnych služieb (5), prerušenie rozsiahlych primárnych služieb (7), úplná strata všetkých služieb (9) Strata zodpovednosti – Dajú sa činy agentov hrozieb vysledovať k jednotlivcovi? Plne vysledovateľné (1), prípadne vysledovateľné (7), úplne anonymné (9)
Business Impact Factors	Finančná škoda - Koľko finančných škôd spôsobí vykorisťovanie? Menej ako náklady na odstránenie zraniteľnosti (1), malý vplyv na ročný zisk (3), významný vplyv na ročný zisk (7), konkurz (9) Poškodenie dobrého mena - Viedlo by zneužitie k poškodeniu dobrého mena, ktoré by poškodilo firmu? Minimálna škoda (1), Strata hlavných účtov (4), strata dobrého mena (5), poškodenie značky (9) Nesúlad – akú mieru vystavenia spôsobuje nesúlad? Menšie porušenie (2), jasné porušenie (5), porušenie s vysokým profilom (7) Porušenie ochrany osobných údajov - Koľko osobne identifikovateľných informácií by sa mohlo zverejniť? Jeden jednotlivec (3), stovky ľudí (5), tisíce ľudí (7), milióny

	ľudí (9)

Určovanie miery rizika

V tomto kroku sa odhad pravdepodobnosti a odhad vplyvu spoja, aby sa vypočítala celková závažnosť tohto rizika. To sa robí zistením, či je pravdepodobnosť nízka, stredná alebo vysoká, a potom urobte to isté pre vplyv. Stupnica od 0 do 9 je rozdelená do troch častí:

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Obrázok 6 Stupnica na určovanie miery rizika

Klasifikácia rizík je v HackMeBank určovaná podľa nasledujúcej tabuľky:

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Obrázok 7 Tabuľka s klasifikáciou rizík

Na určovanie miery rizika v HackMeBank slúži pomôcka v aplikácii Excel s názvom Risk Assessment Calculator. Za udržiavanie tejto aplikácie zodpovedá manažér kybernetickej bezpečnosti.

b) zabezpečuje, aby opakované hodnotenia rizika informačnej bezpečnosti priniesli konzistentné, platné a porovnateľné výsledky;
c) identifikuje riziká informačnej bezpečnosti:
- uplatňuje proces hodnotenia rizík bezpečnosti informácií na identifikáciu rizík spojených so stratou dôvernosti, integrity a dostupnosti informácií v rámci systému riadenia bezpečnosti informácií. Proces identifikácie rizík prebieha počas každej zmeny v aplikácii alebo softvéri.

Za identifikáciu rizík zodpovedá bezpečnostný manažér, resp. Ním určený bezpečnostný analytik.

Zoznam aktív a vlastníkov

Zoznam aktív a vlastníkov je uvedený v nasledujúcej tabuľke:

Názov aktíva	Meno vlastníka	Hodnota aktíva	Dostupnosť	Integrita	Dôvernosť
Office 365	Jano	10 000 Eur	Vysoká	Nízka	Stredná
CORE system	Fero	100 000 Eur	Vysoká	Vysoká	Vysoká
CCDB	Zuzka	50 000 Eur	Vysoká	Stredná	Stredná
IDP	Karol	10 000 Eur	Vysoká	Vysoká	Stredná
Digitálne kanály	Gertrúda	50 000 Eur	Vysoká	Vysoká	Stredná
Hardvér DC	Jano	100 000 Eur	Vysoká	Vysoká	Stredná
Hardvér používatelia	Jano	20 000 Eur	Vysoká	Vysoká	Stredná
Budova DC	Karol	2 000 000 Eur	Vysoká	Vysoká	Stredná

d) analyzuje riziká informačnej bezpečnosti:
- posudzuje možné dôsledky, ktoré by viedli, ak by sa naplnili riziká
- posudzuje reálnu pravdepodobnosť výskytu rizík
- určuje úrovne rizika;

Hodnotenia rizika

Organizácia uchováva zdokumentované informácie o procese hodnotenia rizika informačnej bezpečnosti. Výsledky hodnotenia rizík sú súčasťou projektovej dokumentácie každého projektu.
Nositeľom rizika je aplikačný vlastník systému.

P.č.	Aktívum	Hrozba	Zraniteľnosť	P	D	R	Akceptovateľné	Vlastník rizika	Mitigácia	P(r)	D(r)	R(r)
1	CORE system	S.T.R.I.D.E	0D, IJ	M	M	M	Nie	Fero	Duálna kontrola, Auditovanie	M	L	L
2	CORE system	S.T.R.I._.E	VL	M	M	M	Nie	Fero	Vybudovanie interného dev tím	L	L	L
3	Digitálne kanály	S.T.R.I.D.E	SM	M	M	M	Nie	Gertrúda	Pravidelné pentesty	L	M	L
4	Hardvér používateľa	S.T.R.I._._	LOD	L	L	L	Áno	Jano				
5	CCDB	S.T.R.I._.E	VL, ID, IAF	M	H	H	Nie	Zuzka	Výmena platfor	M	M	M

									my, šifrovanie dát			
6	IDP	S.T.R.I.D.E	VL, CF, IJ, ID, SM,VOC,IAF,SDIF, 0D,	M	M	M	Nie	Karol	Výmena IDP	L	L	L
7	Hardvér DC	_._._._.D._	FI	L	H	M	Nie	Jano	Školenia, Hasiace prístroje,	L	M	L
8	Budova DC	_._._._.D._	ND	L	H	M	Nie	Jano	Vybudovanie redundandného DC	L	L	L
9	Office 365	S.T.R.I.D.E	VL	M	L	L	Áno	Gertrúda				
10	Digitálne kanály	S.T.R.I.D.E	RCH	M	M	M	Áno	Gertrúda	Zmena app architektúry	M	L	L

Komunikácia

Interná komunikácia

V HackMeBank je povolená interná aj externá komunikácia nasledovne:

- Z Desktopov a notebookov je povolené komunikovať len pomocou O365 aplikácií (MS Outlook, MS Teams)
- Z mobilných telefénov pomocou O365 aplikácií a aplikácii používajúce GSM siete (SMS)

Zapojenie externých subjektov do komunikácie (napr. Preposlanie pozvánok na stretnutia v MS Teams) podlieha schváleniu security manažéra. Pri predložení žiadosti je potrebné zabezpečiť podpísanie NDA s externým subjektom. Po skončení platnosti zmluvy alebo účelu (napr. Ukončenie výberového konania) je potrebné zakázať prístup externého subjektu do spoločnej komunikácie (odobratie domény externej spoločnosti na O365).
Povolenie internej aj externej komunikácie v inom komunikačnom kanáli podlieha schváleniu security manažérom a útvaru Compliance (kontrola súladu s požiadavkami regulátorov, napr. MIFID).

Komunikácia s verejnosťou a médiami

Komunikácia s verejnosťou je dovolená len hovorcovi HackMeBank a vyjadrenia hovorcu podliehajú schvaľovaniu Predstavenstvom.

Komunikácia cez sociálne siete je dovolená len oddeleniu Marketingu v autorizovaných sociálnych sieťach a pomocou účtov v sociálnych médiách zaregistrovaných na banku (nie fyzické osoby).
Stratégia komunikácie v sociálnych sieťach je schvaľovaná v rámci stratégie HackMeBank na obmedzené časové obdobie a je riadená priamo riaditeľom oddelenia Marketingu.

Komunikácia s IT oddelením

Na komunikáciu s IT oddelením je možné použiť len autorizované kanály.
Na zadávanie požiadaviek na IT oddelenie je dovolené používať nasledovné komunikačné kanály:

- JIRA ServiceDesk
  - v pracovných dňoch 8-17:00
- Telefónne číslo 0905123456
  - pohotovostné číslo mimo pracovných hodín
  - komunikácia pri strate alebo poruche zariadení

Komunikácia s klientami

Komunikácia s klientami je v kompetencii oddelenia Callcentra. Callcentrum používa nasledovné komunikačné kanály:

- emailovú adresu callcentrum@hackme.bank
- telefónne číslo callcentra 02123456
- inbox v mobilnej aplikácii (smart banking)

V prípade nedostupnosti služieb pre klientov je komunikácia presmerovaná na statické webové stránky s upozornením o nedostupnosti služieb a pokynmi pre klientov.
Použitie akéhokoľvek komunikačného kanálu je zakázané.

Vyhlásenia o použiteľnosti - SoA

"Organizácia vypracuje vyhlásenie o použiteľnosti'"
V tejto kapitole je uvedená mapa implementácie systémov riadenia informačnej bezpečnosti pre niektoré kapitoly (ISO/IEC 27001).
HackMeBank sa zaväzuje revidovanie týchto kapitol minimálne 1 X ročne. Za revidovanie zodpovedá manažér informačnej bezpečnosti a certifikačný orgán.

A.6 Organization of information security

A.6.1 Internal organization

A.6.1.3 Kontakt s orgánmi

V tejto kapitole je uvedené, ako HackMeBank udržiava kontakt s príslušnými orgánmi.

Národná banka Slovenska (NBS)

Komunikácia s NB Slovenska prebieha pomocou portálu NBS. Do portálu má prístup štatutár banky a osoby z právneho oddelenia poverené štatutárom (viď kapitola Organizačná struktúra).

Európska centrálna banka (ECB)

Komunikácia s ECB Slovenska prebieha pomocou portálu NBS. Do portálu má prístup štatutár banky a osoby z právneho oddelenia poverené štatutárom (viď kapitola Organizačná struktúra).

Polícia Slovenskej republiky

S políciou SR môže komunikovať len právne oddelenie s predchádzajúcim súhlasom Predstavenstva HackMeBank.

A.6.2.1 Pravidlá pre mobilné zariadenia

HackMeBank má zavedenú politiku a bezpečnostné opatrenia na riadenie rizík spojených s používaním mobilných zariadení. HackMeBank používa nasledovné typy mobilných zariadení: notebooky, tablety, mobilné telefóny.

Registrácia mobilných zariadení

Za registráciu mobilných zariadení zodpovedá oddelenie IT.

Fyzická ochrana mobilných zariadení

Každý používateľ je zodpovedný za ochranu nemu zverených mobilných zariadení. Všetky mobilné zariadenia sú poistené a zamestnanec je povinný v prípade poistnej udalosti spolupracovať v poistnej udalosti a znáša náklady na spoluúčasť.
Stratu alebo poškodenie mobilného zariadenia je zamestnanec povinný hlásiť na IT oddelenie.

Obmedzenia pri inštalácii softvéru

Používateľ mobilného zariadenia môže používať zariadenie len v rámci práv, ktoré mu boli pridelené oddelením IT. Akokoľvek neautorizovaná zmena oprávnením je považovaná za bezpečnostný incident.

Verzie softvéru mobilných zariadení

Používateľ mobilného zariadenia je povinný riadiť sa pokynmi oddelenia IT s cieľom udržiavať zariadenie v aktuálnej verzii SW.

Obmedzenie pripojenia k informačným službám

Používatelia nemajú obmedzenia na pripojenia k informačným systémom HackMeBank.

Kontroly prístupu

Všetky prístupy do informačného systému HackMeBank sú logované a reportované nadriadeným zamestnancom.

Kryptografické techniky

Na pripojenie k informačným systémom HackMeBank je zakázané používanie nešifrovaných protokolov.

Ochrana pred škodlivým softvérom

Zariadenia pre používateľov sú chránené pomocou antivírusového systému, ktorý je v správe IT oddelenia. Každá identifikácia škodlivého kódu je riešená ako bezpečnostný incident.

Servery sú chránené antivírusovým systémom len v prípade, ak spracovávajú dáta ktoré poslali klienti priamo na server.

Diaľkové vypnutie, vymazanie alebo uzamknutie

Prípade straty zariadenia je IT oddelenie povinné zmazať všetky klasifikované dáta. Klasifikácia dát je detailnejšie popísaná v kapitole 8.2. Klasifikácia informácií.

Zálohy

Každý systém a vypracovaný plán záloh, za realizáciu zodpovedá technický vlastník systému. Pre všetky plány záloh platia požiadavky na retenciu podľa nasledujúcej tabuľky.

Klasifikácia dát	Cyklus zálohovania	Retencia
Verejné	Len pri zmene	3 mesiace
Interné	Pri zmene, minimálne 1 X za mesiac	1 rok
Tajné	Pri zmene, minimálne 1 X za deň	3 roky
Prísne tajné	Pri zmene, minimálne 1 X za hodinu	10 rokov

Používanie webových služieb a aplikácií

A.7 Bezpečnosť ľudských zdrojov

A.7.1 Pred nástupom do zamestnania

A.7.1.1 Skríning

U všetkých uchádzačov o zamestnanie do HackMeBank sa vykonávajú previerky v súlade s legislatívou a etikou, tzv. skríning. Dôvodom skríningu je predísť interným podvodom.

Proces skríningu v HackMeBank obsahuje nasledovné kritériá a obmedzenia:
- za výkon skríningu zodpovedá HR oddelenie a security manažér. HR oddelenie sa na túto činnosť môže prenajať externú firmu.
- skríning prebieha v závere prijímacieho konania
- proces skríningu umožňuje zamietnuť úspešného kandidáta.

Uchádzači o zamestnanie (vrátane dodávateľov) sú povinní doručiť na HR oddelenie:

- životopis uchádzača s uvedením:
  - telefonických kontaktov na predchádzajúcich zamestnávateľov;
  - kontakt na organizácie, ktorá uchádzačovi vydali certifikáty o odbornej spôsobilosti;
- notárom overené potvrdenie o akademickej a odbornej kvalifikácii;
- výpis z registra trestov nie starší ako 3 mesiace;
- odporúčanie od posledného zamestnávateľa suvedením kontaktu na HR oddelenie;

A.7.1.2. Podmienky zamestnania

NDA

Všetci zamestnanci HackMeBank, ktorí majú prístup k dôverným informáciám, musia pred prístupom k informáciám podpísať dohodu o mlčanlivosti (ďalej NDA). NDA obsahuje nasledovné informácie:
- zákonné povinnosti a práva zamestnanca (napr. pokiaľ ide o autorské právo, súkromie a ochranu osobných údajov atď.)

- zodpovednosť za klasifikáciu informácií a riadenie organizačného majetku, s ktorým narába zamestnanec alebo dodávateľ;
- opatrenia, ktoré môže organizácia podniknúť v prípade, že zamestnanec nerešpektuje bezpečnostné požiadavky.

Kontroly sú úmerné citlivosti informácii, ku ktorým má zamestnanec pristupovať, súvisiacim rizikám a obchodným požiadavkám HackMeBank.

Autorské pravá zamestnanca

Zamestnanec HackMeBank má právo na ochranu osobných údajov a súkromia. Zamestnanec má právo mať všetky svoje osobné údaje chránené pred neoprávneným použitím a ochrana súkromia je vyhradená.
Zamestnanec HackMeBank má právo na ochranu autorských práv. Zamestnanec má právo mať svoje diela a výtvory chránené pred neoprávneným kopírovaním a používaním.
Zamestnanec HackMeBank má právo mať prístup k informáciám o rizikách. Zamestnanec má právo na informácie o možných ohrozeniach bezpečnosti, ktoré môžu ohroziť jeho osobné údaje a autorské práva.

Zodpovednosť za klasifikáciou informácií

Zodpovednosť za klasifikáciu informácií v HackMeBank nesie aplikačný vlastník. Klasifikácia informácií prebieha počas zápisu do interného systému HackMeBank.
Technická realizácia klasifikácie údajov v HackeMeBank prebieha pomocou nástrojov balíka Office 365.
V prípade prístupu ku klasifikovaný údajom neoprávnenou osobou je povinnosťou zamestnanca založiť bezpečnostný incident a zadať jeho riešenie DPO (Data privacy officer).

Opatrenia v prípade nerešpektovania bezpečnostných požiadaviek

V prípade nerešpektovania bezpečnostných požiadaviek ma zamestnávateľ právo prijať opatrenia v zmysle pracovnej zmluvy zamestnanca.

A.7.3. Ukončenie alebo zmena pracovného pomeru

HackMeBank má definované a informuje svojich zamestnancov a svojich dodávateľov o ich povinnostiach a zodpovednostiach súvisiacich s informačnou bezpečnosťou, ktoré zostávajú v platnosti aj po ukončení alebo zmene ich pracovného pomeru.
Nesprávne ukončenie alebo zmena zamestnania môžu spôsobiť bezpečnostné problémy. Môže viesť k tomu, že jeho prístupové práva, ktoré majú prístup k citlivým informáciám, zostanú nechránené a môžu byť zneužité. Ak sa zamestnanec rozhodne odísť a organizácia nemá implementované dostatočné opatrenia, môže si odniesť citlivé informácie a využívať ich napr. pre svoje vlastné účely.

A.7.3.1. Ukončenie alebo zmena pracovných povinností

Odstránenie logických a fyzických prístupových práv

Za odstránenie prístupových práv po ukončení pracovného vzťahu zodpovedá nadriadený zamestnanca. Nadriadený zadáva štandardnú požiadavku na IT oddelenie a uvedie zoznam všetkých systémov, do ktorých mal zamestnanec prístup.

Vrátenie vybavenia, ktoré patrí organizácii

Zamestnanec odovzdáva pridelený hardware v deň odchodu zo zamestnania IT oddeleniu oproti odovzdávaciemu protokolu.

Mlčanlivosť

Zamestnanec je po odchode zo zamestnania povinný dodržiavať mlčanlivosť. Povinnosť mlčanlivosti zamestnanca zakotvuje § 81 písm. f) Zákonníka práce nasledovne: „Zamestnanec je povinný najmä zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvedel pri výkone zamestnania a ktoré v záujme zamestnávateľa nemožno oznamovať iným osobám; povinnosť mlčanlivosti sa nevzťahuje na oznámenie kriminality alebo inej protispoločenskej činnosti.“
V špeciálnych prípadoch je možné aj uzavretie samostatnej dohody o mlčanlivosti (NDA). V prípade prijatia takejto dohody by zamestnanec, ktorý dohodu prijal bol viazaný povinnosťou mlčanlivosti aj po skončení pracovného pomeru.

A.8 Asset management

A.8.1. Zodpovednosť za majetok

A.8.1.1. Inventarizácia majetku

Pod pojmom aktíva sa označuje všetko, čo vlastní HackMeBank – jej majetok. Je to všetko, čo spoločnosť nadobudla minulými aktivitami a od čoho sa očakáva, že prinesie ekonomický úžitok v budúcnosti.
Za správu a aktualizáciu fyzických aktív pre používateľov (notebooky, tablety, desktopy) je zodpovedné IT oddelenie.
Pri správe je IT oddelenie povinné viesť nasledujúce informácie:

Typ informácie	Popis	Poznámka
HW ID, SW ID	Identifikátor HW alebo SW	Hostname zariadenia, názov SW
Umiestnenie	Lokalita, v ktorej sa používa zariadenie alebo softvér	HQ (Head quater), pobočka a pod.
Výrobca	Výrobca zariadenia	Dell, HP, Microsoft a pod.
Model	Model zariadenia alebo verzia SW	Latitude E820
Sériové číslo	Sériové čislo zariadenia alebo licencie	AS123456
Inventárny štítok	Informácia o zariadení	HMB123456

Za dokumentáciu k fyzickým aktívam pre používateľov a jej aktualizáciu zodpovedá IT oddelenie. Súčasťou dokumentácie je aj plán kontinuity činnosti. Plán musí obsahovať informácie o činnosti, ktorú musí organizácia alebo používateľ urobiť v prípade nedostupnosti HW a SW, viď nasledujúca tabuľka.

Typ assetu	Popis udalosti	Povinnosť vlastníka
HW	Strata alebo nefunkčnosť HW	Kontaktovať IT oddelenie

Office 365	Nedostupnosť služieb	Kontaktovať IT oddelenie

A.8.1.2. Vlastníctvo majetku

Každý majetok má svojho vlastníka, tzv. vlastníka aktíva. Vlastník je povinný

- zahrnúť majetok do inventára, viď inventarizácia majetku,
- zabezpečiť primeranú ochranu podľa typu majetku (HW, SW a pod.),
- definovať a kontrolovať obmedzenia prístupu k aktívu,
- zabezpečiť správne zaobchádzanie.

A.8.1.3. Správne využitie majetku

Každý vlastník aktíva je povinný pripraviť pracovný postup pre používateľa, v ktorom je popísané správne používanie aktíva.
Nedodržiavanie tohto manuálu musí byť vyhodnotené ako porušenie pracovného postupu. Pri zistení nedodržiavania pracovných postupov a identifikácii neoprávneného prístupu k údajom je potrebné zadať bezpečnostný incident.

A.8.1.4. Vrátenie majetku

Zamestnanec odovzdáva pridelený majetok v deň odchodu zo zamestnania oproti odovzdávaciemu protokolu. Odovzdanie vlastníctva informácií alebo knowhow je platné momentom odobratia prístupu zamestnancovi k aplikácii.

A.8.2. Klasifikácia informácií

V nasledujúcej tabuľke sú uvedené kritéria pre klasifikáciu dát.

Klasifikačný stupeň	Dopad pri strate	Skratka
Verejné	Zverejnenie nespôsobuje žiadnu škodu.	P
Interné	Zverejnenie spôsobí menšie rozpaky alebo menšie prevádzkové ťažkosti.	I
Tajné	Zverejnenie má významný krátkodobý vplyv na operácie alebo taktické ciele.	C
Prísne tajné	Zverejnenie má vážny vplyv na dlhodobé strategické ciele alebo ohrozuje prežitie organizácie.	SC

V procese klasifikácie platia zároveň nasledujúce pravidlá:

- dáta neoznačené klasifikačným stupňom sa považujú za Tajné
- v prípade, že dataset obsahuje viaceré klasifikačné stupne, tak pre celý dataset platí najvyšší klasifikačný stupeň z kvalifikátorov

A.8.2.2. Označovanie informácií

Každý dokument musí obsahovať informáciu o klasifikačnom stupni, ktorá je umiestnená na viditeľnom mieste v päte dokumentu.

Ak dokument neobsahuje informáciu o klasifikácii, aplikačný vlastník je povinný doplniť klasifikačný stupeň do dokumentu alebo jeho kópie.

A.8.2.3. Nakladanie s majetkom

Pre každý klasifikačný stupeň platia obmedzenia prístupu pre každú úroveň utajenia, viď. Nasledujúca tabuľka.

Klasifikačný stupeň	Určené pre	Udeľovanie výnimky
Verejné	Bez obmedzenia	
Interné	Všetci zamestnanci a 3tie strany vo vzmluvnom vťahu k HackMeBank	Aplikačný vlastník
Tajné	Len definované role	Aplikačný vlastník
Prísne tajné	Len definované role	Aplikačný vlastník + Predstavenstvo

Všetky kópie záloh (dočasné aj trvalé) podliehajú rovnakým pravidlám ochrany ako originály. Za kontrolu výmazu záloh je zodpovedný aplikačný vlastník, výkon realizuje IT oddelenie.

Dáta sú archivované podľa stupňa klasifikácie, zmena stupňa utajenia alebo zničenie dát je možná len so súhlasom vlastníka dát.

A.8.3. Manipulácia s médiami

A.8.3.1. Správa vymeniteľných médií

Pre správu vymeniteľných médií sú implementované nasledujúce kontroly:

- Používanie vymeniteľných médií je možné len iba v prípade, že na to existuje obchodný dôvod. Postup pridelenia médiá prebieha nasledovne:
  - Zamestnanec požiada o vymeniteľné médium
  - Žiadosť schváli nadriadený zamestnanca
  - IT oddelenie pridelí vymeniteľné médium zamestnancovi
  - Zamestnanec aktivuje médium pomocou softvéru nainštalovanom na jeho zariadení, ktoré mu vygeneruje unikátny PIN k médiu
  - Zamestnanec používa vymeniteľné médium spolu s PINom
- Zamestnanec skladuje autorizované médiá v bezpečnom a zabezpečenom prostredí;
- V prípade straty alebo poškodenia vymeniteľného média je zamestnanec povinný komunikovať s IT oddelením, ktoré určí ďalší postup.
- V prípade zálohovania a archivácie dát musí IT oddelenie zvážiť používanie viacero kópií cenných informácií na samostatných médiách a vo viacerých lokalitách.

A.8.3.2. Likvidácia médií

Likvidácia médií prebieha v HackMeBank v spolupráci s externou organizáciou s certifikáciou na prácu a likvidáciu s klasifikovanými dátami.
Zamestnanci sú povinný riešiť likvidáciu s IT oddelením HackMeBank, ktoré zabezpečí likvidáciu cez zmluvného partnera.

A.8.3.3. Fyzický prenos médií

Zamestnanec je povinný používať vymeniteľné médiá s vhodným obalom na ochranu obsahu pred fyzickým poškodením a ochranu pred environmentálnymi faktormi - ako sú teplo alebo elektromagnetické polia.
Šifrovací kľúč zamestnanec nikdy nesmie posielať spolu so šifrovanými údajmi.

A.9 Kontrola prístupu

A.9.1. Obchodné požiadavky na riadenie prístupu

A.9.1.1. Politika kontroly prístupu

Pred každou **implementáciou obchodnej aplikácie** by mali byť implementované nasledovné bezpečnostné požiadavky:

a) Silné autentifikačné mechanizmy, ako sú heslá, čipové karty alebo biometrické údaje.
b) Šifrovať všetky klasifikované dáta uložené v databázach.
c) Implementovať dostatočné mechanizmy pre správu prístupových práv.
d) Monitorovať a logovať všetky prístupy používateľov, administrátorov aj technických účtov.
e) Implementovať firewally a dostatočne silné kryptografické protokoly pre zabezpečenie sieťovej komunikácie.
f) Zabezpečiť, aby boli aplikácie a vždy aktualizované.
g) Implementovať bezpečný spôsob vzdialenej správy systémov.

Konzistentnosť medzi prístupovými právami a klasifikáciou informácií je dôležitá. Prístupové práva by mali byť nastavené tak, aby zodpovedali klasifikácii informácií. To znamená, že by mali byť pridelené práva len na základe potreby na získanie informácií. Prístupové práva by mali byť nastavené tak, aby bola zabezpečená príslušná úroveň bezpečnosti pre každú úroveň klasifikácie informácií.

Všetky aplikácie a procesy musia dodržiavať nasledujúce **právne predpisy a zmluvné záväzky** týkajúce sa obmedzenia prístupu k údajom alebo službám:
- Zákon o ochrane osobných údajov
- GDPR
- Interné predpisy
- Interná bezpečnostná politika
- Zákon o bankách
- PSD2

Oddelenie rolí, ktoré sa týkajú kontroly prístupu, je zabezpečené pomocou nasledujúcich administrátorských rolí:

a) Správca prístupu: zodpovedá za evidenciu prístupu používateľov do informačných systémov, za zabezpečenie prístupu len oprávneným používateľom a za správu identifikátorov prístupu.

b) Auditor: vykonáva audit prístupu a overuje, či boli bezpečnostné prístupové opatrenia dodržané.
c) Správca bezpečnosti: zabezpečuje, aby boli všetky zásady prístupu dodržiavané.
d) Systémový správca: zodpovedá za správu a údržbu systémov vrátane oprávnení prístupu.

Počas pravidelnej **kontrola prístupových práv** je potrebné vykonávať tieto činnosti:

a) Vytvárať a implementovať postupy a kontroly na zabezpečenie účasti všetkých relevantných účastníkov, t.j. všetky prístupy musia byť autorizované aplikačným vlastníkom.
b) Identifikovať ľudí, ktorí majú prístup k informačným systémom alebo údajom, t.j. všetky požiadavky musia byť manažované pomocou interného požiadavkového systému.
c) Udržiavať zoznamy prístupových práv a zabezpečiť ich aktualizáciu podľa potreby. Za aktualizáciu zodpovedá aplikačný vlastník a výkon realizuje IT oddelenie.
d) Udržiavať zoznamy prístupových práv na zariadeniach pre všetkých zamestnancov a externých pracovníkov je v zodpovednosti IT oddelenia.
e) Udržiavať záznamy o všetkých zmenách prístupových práv je v zodpovednosti oddelenia IT bezpečnosti.
f) Monitorovať prístup k informačným systémom a údajom je v zodpovednosti oddelenia IT bezpečnosti.
g) Zabezpečiť audit prístupu k informačným systémom a údajom je v kompetencii interného audítora.
h) Vykonávať pravidelné revízie prístupových práv minimálne 1 X ročne.

Počas odstránenia prístupových práv je potrebné:

a) Identifikovať prístupové práva, ktoré je potrebné odstrániť.
b) Preveriť všetky akreditácie a oprávnenia, ktoré súvisia s prístupovými právami.
c) Zablokovať prístupové práva podľa potreby.
d) Zaznamenať informácie o odstránení prístupových práv.
e) Odoslať oznámenie o odstránení prístupových práv zodpovedným osobám.
f) Monitorovať a revidovať prístupové práva podľa potreby.

Je potrebné monitorovať všetky **roly, ktoré majú privilegovaný prístup** :

a) administrátori systému,
b) tímoví lídri,
c) vývojári,
d) skúšobní inžinieri,
e) technici
f) ďalší používatelia, ktorí majú prístup k dôležitým informáciám alebo systémom.

A.9.1.2. Prístup k sieťam a sieťovým službám

V HackMeBank existuje niekoľko **sietí a sieťových služieb**, ku ktorým je povolený prístup:

a) Cloudové služby SaaS, PaaS a IaaS
b) Prístup k internetu

c) E-mailové služby
d) Správa sieťových zariadení
e) Virtuálne súkromné siete (VPN)

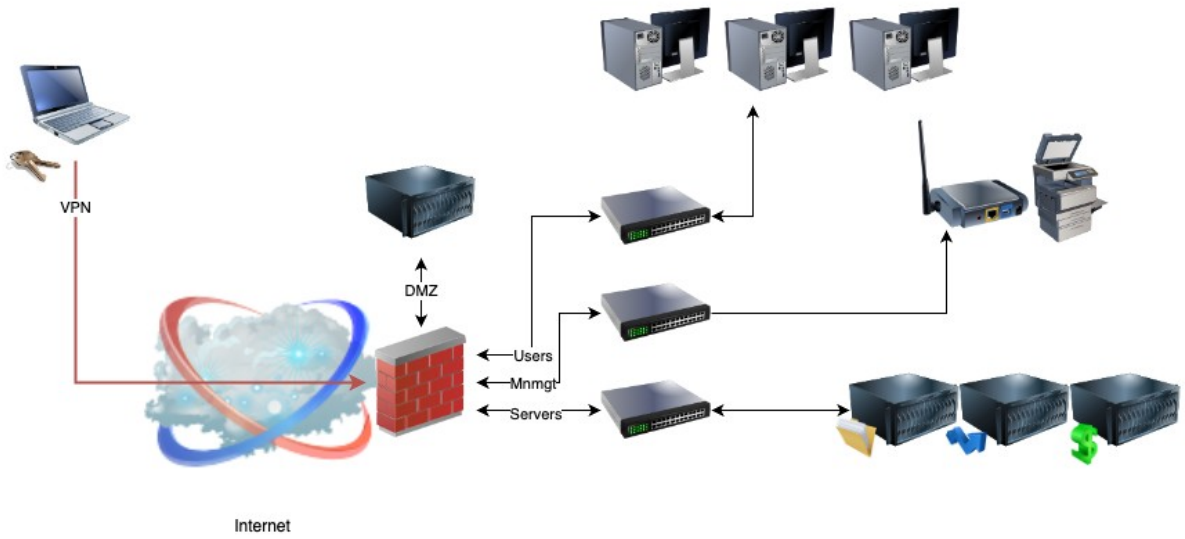
Administrátzor by mal dodržiavať nasledovné **autorizačné postupy** na určenie toho, kto má povolený prístup ku ktorým sieťam a službám:

a) Definuje zoznam zdrojov prístupu, ktoré je potrebné mať prístupné.
b) Definuje kritériá pre prístup k týmto zdrojom (napr. prístupové úrovne, oprávnenia a povolenia).
c) Definuje procesy pre udeľovanie oprávnení a povolení pre prístup k týmto zdrojom.
d) Definuje procesy pre audit oprávnení a povolení a prístupu k zdrojom.
e) Definuje procesy pre zabezpečenie, že oprávnenia a povolenia sú uzamknuté po ukončení prístupu.
f) Definuje postupy pre prípadné zrušenie oprávnení a povolení.

Kontroly na ochranu prístupu k sieťam a službám zahŕňajú:

a) Identifikácia a autentifikácia používateľov – určenie a overovanie identity používateľov pri prístupe k sieťam a službám. To môže byť dosiahnuté pomocou hesiel, číselných alebo biometrických identifikátorov.
b) Prístupové práva – stanovenie prístupových práv k sieťam a službám pre jednotlivých používateľov.
c) Kontrola prístupu – zavedenie mechanizmov na kontrolu prístupu používateľov k sieťam a službám.
d) Rozdeľovanie úloh – priradenie konkrétnych úloh jednotlivým používateľom a stanovenie prístupových práv pre každú úlohu.
e) Správa prístupových práv – monitorovanie a revízie prístupových práv, aby sa zabezpečilo, že sú vyhradené pre príslušných používateľov.
f) Záznamy o prístupe (logovanie) – vytvorenie záznamov o prístupe k sieťam a službám, aby sa zistilo, kto pristupoval k čomu a kedy.

Do **sietí a sieťových služieb sa pristupuje** nasledovne:
Priamy prístup do siete (lokálna sieť) sa realizuje pomocou označeného sieťového kábla, ktorý je pripojený do prepínača.
Vzdialený prístup je umožnený pomocou VPN pripojenia.
Akýkoľvek iný prístup je zakázaný a požiadavky musia byť konzultované s IT oddelením.



Obrázok 8 Rozdelenie sietí v HackMeBank

Prístup k sieťam a službám je možný len po multi-faktorovom overení používateľa:

a) Overenie doménového účtu používateľa, resp. Pomocou VPN klienta s SSO
b) Overenie 2-hého faktora pre prihlásenie (Office365 Authenticator)

Za monitorovanie a využívanie sieťových služieb zodpovedá IT oddelenie, resp. Poskytovateľ internetového pripojenia.

A.9.2. Správa používateľských prístupov

A.9.2.1. Registrácia a zrušenie registrácie používateľa

V HackMeBank je riadenie identit realizované nasledujúcimi číselníkmi:

Zamestnanci:

Názov systému	Doménový účet	Lokálne ID	Iné
Office 365	X		
Core system		X	
VPN koncentrátor	X		
Wifi AP			Lokálny účet
CRM	X		
DWH	X		

Klienti

Názov systému	Klientský účet	Master ID klienta	Iné ID
Mobile banking	X		
Core system		X	
Broker			Lokálny účet
CRM		X	

DWH	X		

A.9.2.2. Poskytovanie prístupu používateľov

- Za schválenie alebo zrušenie prístupových práv k užívateľským ID je zodpovedný vlastník informačného systému.
- prístupové práva by sa nesmú aktivovať pred autorizáciou. Za aktiváciu je zodpovedné IT oddelenie po predchádzajúcej kontrole potrebných súhlasov.
- aplikačný vlastník je zodpovedný za evidenciu centrálneho záznamu prístupových práv udelených každému ID užívateľa. Technickú realizáciu zabezpečuje IT oddelenie.
- dynamicky sa meniace prístupové práva (napr. Developeri a testeri) si môžu požiadať o rolu „Admin for a day“, t.j. na základe požiadavky im je povolený prístup do konca pracovnej doby.

A.9.2.4. Správa tajných overovacích informácií používateľov

Pri výmene dát s klasifikáciou Prísne tajné si používatelia vymieňajú heslá iným komunikačným kanálom ako tým, ktorým sa vymieňa šifrovaný materiál, napr. Email + SMS.

A.9.2.5. Kontrola prístupových práv používateľov

Kontroly prístupových práv musia byť realizované podľa nasledujúcej tabuľky:

Stupeň klasifikácie	Po každej zmene	Mesačne	Ročne
Verejné			X
Interné			X
Tajné		X	
Prísne tajné	X		X

A.9.2.6. Odobratie prístupových práv používateľom

Za odobratie prístupových práv zodpovedá nadriadený zamestnanec, výkon realizuje IT oddelenie, viď RACI matica.

Typ	Responsible	Accountable	Consult	Inform
Vedúci zamestnanca	X			
Aplikačný vlastník			X	
IT oddelenie		X		
IT bezpečnosť				X

A.9.3. Povinnosti používateľov

A.9.3.1. Použitie tajných overovacích informácií

- používatelia musia absolvovať min. 1X ročne e-learningové školenie na hesiel;
- na uchovávanie hesiel musia používatelia používať aplikáciu Keepass ;
- heslá musia mať minimálne 12 znakov, nesmú obsahovať meno, dátum

Narodenia a nesmú byť náchylné na slovníkový útok.

A.9.4. Kontrola prístupu do systému a aplikácií

A.9.4.1. Obmedzenie prístupu k informáciám

Prístup do každej aplikácie musí byť autorizovaný aplikačnou rolou používateľa, ktorá definuje maticu oprávnení prístupu ku klasifikovaným dátam.
Za prípravu matice oprávnení je zodpovedný aplikačný vlastník.

A.9.4.2. Bezpečné prihlasovacie postupy

Ku každej aplikácii existuje manuál, ktorý obsahuje postup prihlásenia. Za prípravu manuálu je zodpovedný aplikačný vlastník.

A.9.4.3. Systém správy hesiel

Všetky systémy musia spĺňať nasledovné požiadavky na správu hesiel:

a) umožniť používateľom vybrať a zmeniť svoje vlastné heslá a zahrnúť postup potvrdenia;
b) presadzovať výber kvalitných hesiel pomocu politík na backende;
c) prinútiť používateľov, aby si pri prvom prihlásení zmenili svoje heslá;
d) vynucovať pravidelné zmeny hesla a podľa potreby;
e) uchovávať záznamy o predtým použitých heslách a zabrániť opätovnému použitiu minulých hesiel;
f) nezobrazovať heslá na obrazovke pri zadávaní;
g) ukladať súbory hesiel oddelene od systémových údajov aplikácie;
h) ukladať a prenášať heslá v chránenej forme.

A.9.4.5. Prístup k zdrojovému kódu programu

Zdrojové kódy sú klasifikované stupňom klasifikácie „Tajné“ a prístup developerov musí byť riadený. Každá zmena kódu musí byť autorizovaná vlastníkom aplikácie, informačnou bezpečnosťou a IT oddelením. Počas kontroly sa zameriavajú hlavne na:

- autorizáciu komponentov 3-tích strán
- testovanie funkčných požiadaviek
- bezpečnosť kódu.

A.11 Fyzická a environmentálna bezpečnosť

A.11.1.1. Fyzický bezpečnostný obvod

Každý perimeter obsahuje kontrolné stanoviská, na ktorých sa musí každá osoba identifikovať. Používanie iných ako oficiálnych perimetrov je zakázané.

Ochrana obvodov – dverí, okien, striech, stien, podláh je realizovaná prevádzkovateľom budovy. Používatelia majú zakázané akokoľvek meniť ochranné prvky bez predchádzajúceho súhlasu prevádzkovateľa budovy.

Všetky požiarne dvere sú signalizované, monitorované a testované a všetky osoby, ktoré sa nachádzajú v priestoroch HackMeBank sú povinné riadiť sa protipožiarnymi pokynmi.

V HackMeBank nainštalované systémy detekcie votrelcov a neobývané priestory sú vždy alarmované. Spustenie alarmu je riešené vždy ako bezpečnostný incident.

A.11.1.2. Fyzické kontroly vstupu

Zamestnanci sú povinní pri príchode a odchode z priestorov HackMeBank použiť na identifikáciu registračnú kartu zamestnanca. Priložením karty na čítačku zaznamená dátum a čas vstupu a odchodu zamestnanca. Editácia záznamov cez HR systém záznamov je možná len so súhlasom nadriadeného zamestnanca.

V budove sídla HackMeBank je umiestnená recepcia, ktorá slúži na kontrolu fyzického prístupu a zároveň a identifikáciu a registrácia návštev a 3-tích strán. Akákoľvek návšteva osôb bez registrácie je zakázaná. Registrované osoby sa môžu pohybovať po budove len v sprievode zamestnanca banky.

Prístup do oblastí, kde sa spracúvajú alebo uchovávajú dôverné informácie (serverovňa, zasadačky s chráneným dohľadom a pod.) je obmedzený na oprávnené osoby. Pridelenie a odobratie práv pre oprávnené osobe ju možné len so súhlasom vlastníka chránenej oblasti.

Všetky prístupy do chránených aj nechránených oblastí sú zaznamenané a v prípade narušenia sú riešené ako bezpečnostný incident.

Všetci zamestnanci, dodávatelia a externé strany musia nosiť vizuálnu identifikáciu na viditeľnom mieste. V prípade vyzvania sú povinní všetky fyzické osoby poskytnúť identifikáciu k nahliadnutiu.

Zamestnanci externých strán nemajú povolený prístup do oblastí, kde sa spracúvajú dôverné informácie. Porušenie je riešené ako bezpečnostný incident.

Fyzické prístupové práva do oblastí vydávajú maximálne na dobu jedného roka. Po exspirácii je nutné prístup opätovne prehodnotiť a schváliť vlastníkom chránených priestorov.

A.11.1.3. Zabezpečenie kancelárií, izieb a zariadení

Kľúčové zariadenia (serverovňa, tlačiarne, zasadačky a pod.) sú umiestnené tak, aby sa zabránilo prístupu verejnosti. Na vstup je možné použiť len kartičku s pridelenými právami na prístup do chránených priestorov.

Zoznamy osôb a telefónne zoznamy sú dostupné len z pracovných desktopov a po 2-faktorovej autentizácii zamestnanca.

Fyzické telefóny sa automaticky uzamknú po 5 minútach nečinnosti.

A.11.1.4. Ochrana pred vonkajšími a environmentálnymi hrozbami

Ochranu pred zemetrasením, požiarom, záplavami, výbuchmi, občianskymi nepokojmi alebo inými formami prírodných alebo človekom spôsobených katastrof zabezpečuje prevádzkovateľ budovy.
Prevádzkovateľ budovy má na tieto nepredvídateľné situácie zriadené poistenie, ktorého výška plnenia odráža aktuálnu hodnotu majetku nájomcov.

A.11.1.5. Práca v zabezpečených priestoroch

V HackMeBank existujú nasledovné zabezpečené priestory:

- zasadačky
- serverovne
- iné technologické miestnosti (wiring room)

Pre prácu v zabezpečených priestoroch sú platné nasledovné pokyny pre prácu:
- dovnútra zabezpečených priestorov môžu mať prístup len oprávnené osoby a len so súhlasom vlastníka priestorov (schválenej role na prístup);
- zabezpečené priestory sa automaticky zamykajú a prístup je logovaný;
- v zabezpečených priestoroch nie je povolené vyhotovenie fotografického, obrazového a zvukového záznamu.

A.11.2. Zariadenia

A.11.2.1. Vybavenie a ochrana

- zariadenia, v ktorých sa spracúvajú citlivé informácie (servery, tlačiarne, skenery a pod.), sú umiestnené len po registrovanom vstupe do priestorov aby sa znížilo riziko, že si informácie prezrú neoprávnené osoby;
- na zariadeniach ani v chránených priestoroch sú zavedené usmernenia pre jedenie, pitie a fajčenie a návštevníci sú povinní ich dodržiavať;

A.11.2.3. Zabezpečenie kabeláže

Akýkoľvek zásah do kabeláže je možný len so súhlasom prevádzkovateľa budovy. Zmeny v zapojení je možné realizovať len v rozsahu manuálu ku kabeláži. Za prípravu a aktualizáciu manuálu je zodpovedné IT oddelenie.
Ku kabeláži existuje dokumentácia a za aktualizáciu je zodpovedné IT oddelenie.
Všetky zmeny v zapojení musí realizovať IT oddelenie.
Používatelia žiadajú o zmenu v zapojení (napr. Aktivovanie zásuvky na pripojenie do počítačovej siete) cez interný požiadavkový systém.

A.11.2.5. Odstránenie aktív

Akýkoľvek prenos majetku HackMeBank je dovolený len po schválení vlastníkom aktíva. Požiadavky na prenos musia byť schválené v internom požiadavkovom systéme.

A.11.2.7. Bezpečná likvidácia alebo opätovné použitie zariadenia

Likvidáciu zariadení, ktoré uchovávajú klasifikované dáta, realizuje vždy zmluvný partner. Za realizáciu procesu likvidácie (objednanie, odovzdanie) je zodpovedné IT oddelenie.

A.11.2.8. Používateľské zariadenia bez dozoru

Používatelia sú povinní ukončiť aktívne relácie po dokončení alebo ich zabezpečiť heslom. Neuzamknutý počítač je považovaný za hrozbu. Pri porušení musí používateľ absolvovať e-learningové školenie z informačnej bezpečnosti zamerané na ochranu klasifikovaných dát.

Na všetkých počítačoch a mobilných zariadeniach je používateľ povinný používať automatizovaný systém na uzamykanie zariadení. Jeho modifikácia je zakázaná.

A.11.2.9. Čistý pracovný stôl a zásady čistej obrazovky

Používatelia sú povinný dodržiavať nasledovné zásady čistého pracovného stola v priestoroch aj mimo priestorov HackMeBank:
- citlivé alebo kritické obchodné informácie musia byť prednostne zamknuté v trezore, keď nie sú potrebné a najmä keď je kancelária uvoľnená;
- na počítačoch musia byť používatelia odhlásení, keď sa nepoužívajú;
- používanie kamier a záznamových zariadení je zakázané;
- médiá obsahujúce citlivé informácie musia byť po tlači z tlačiarní zlikvidované.

A.12 Operations security

A.12.2. Ochrana pred škodlivým softvérom

A.12.2.1. Kontroly proti malvéru

Používateľom je zakázané inštalovať a používať neautorizovaného softvéru. Za autorizáciu softvéru zodpovedá manažér informačnej bezpečnosti. Porušenie používania autorizovaného SW je riešené v disciplinárnom konaní.

Používatelia sú pri komunkácii so sieťou internetu povinní používať proxy server, na ktorom je implementovaná kontrola podozrivých škodlivých webových stránok a komunikácia je automaticky zakázaná. Používateľ je upozornený o škodlivosti danej stránky a dôvodoch blokovania. Používateľ môže požiadať o výmaz danej stránky zadaním požiadavky cez interný systém.

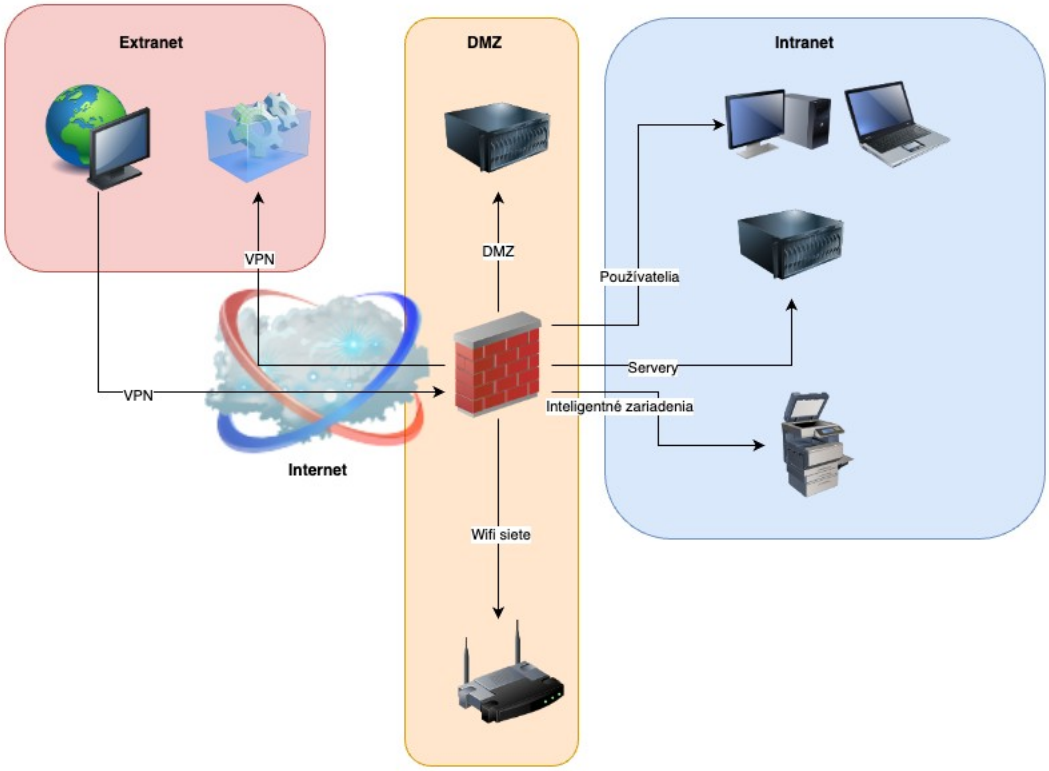
Na každom zariadení, do ktorého má prístup používateľ, je nainštalovaný softvér na detekciu a opravu škodlivého softvéru. Softvér je manažovaný centrálne a pravidelne kontroluje počítače a pripojené médiá. Za prevádzku a reporty zodpovedá IT oddelenie.
Pri identifikácii škodlivého kódu je automaticky zaslaná notifikácia na IT oddelenie a IT oddelenie rieši problém priamo s používateľom (spustením skenovania disku, oddelením od siete, atď.) . Pri hromadnom útoku je odpojená tá časť siete, v ktorej je identifikovaný útok a napadnuté systémy sú vypnuté. Aktivitu riadi IT oddelenie, používateľ sa musí riadiť pokynmi.

HackMeBank je pravidelne informovaná o novinkách o útokoch škodlivého softvéru dodávateľom aplikačných bezpečnostných modulov firewallov, ktorý je zároveň dostupný pri riešení incidentov.

A.13.1.3. Segregácia v sieťach

Počítačová sieť v HackMeBank je rozdelená do domén:
- Intranet
  - lokálna sieť pre desktopy, servery
  - sieť DMZ
  - siete pre mobilné zariadenia
- Extranet
  - siete pre 3-tie strany a dodávateľov
- Internet

- verejná počítačová sieť



Obrázok 9 Náhľad na rozdelení sietí firewallom

Prístupy sú riadené sieťovým firewallom, ktorého prevádzku zabezpečuje IT oddelenie.

Podrobný popis sietí je uvedený v IP pláne, za ktorého aktualizáciu zodpovedá IT oddelenie.

Sieť	Subnet	Povolené masky sietí
Intranet	10.0.0.0/16	24-27
Extranet	192.168.0.0/16, Google cloud, Azure cloudAWS cloud	24
Internet	195.28.1.0/24	X

A.13.2. Prenos informácií

Elektronická komunikácia môže prebiehať len z autorizovaných zariadení – pracovných staníc používateľov.
Servery na komunikáciu HackMeBank sú umiestnené v Office365, kde prebieha aj automatické skenovanie emailov (Exchange) a ukladaných súborov (OneDrive).
Zamestnanci majú zakázané kompromitovať organizáciu (napr. ohováraním, obťažovaním, vydávaním sa za identitu, preposielaním reťazových listov, neoprávneným nákupom). Každý zamestnanec je povinný raz ročne absolvovať interné školenie na Compliance kódex.

Zamestnanci sú povinný šifrovať informácie, ktoré sú klasifikované ako Tajné a Prísne tajné.

Zamestnanci nesmú nechávať citlivé informácie v tlačiarňach alebo faxoch a nesmú viesť dôverné rozhovory na verejných miestach alebo prostredníctvom nezabezpečených komunikačných kanálov.

A.13 Communications security

A.13.1. Správa bezpečnosti siete

A.13.1.1. Sieťové ovládacie prvky

Všetky sieťové domény sú oddelené pomocou sieťového firewallu. O povolenia na komunikáciu na firewalle musí používateľ požiadať formou internej požiadavky a musí ju schváliť vlastník siete, do ktorej chce mať používateľ prístup.

Obvod pre každú doménu by mal byť dobre definovaný a prístup medzi sieťovými doménami by mal byť riadený pomocou brány.
Bezdrôtové siete sú považované za externé pripojenia a preto sú oddelené od interných sietí. Na prístup do bezdrôtovej siete používajú zamestnanci CaptivePortal, v ktorom si zaregistrujú 1 svoje zariadenie.

Kompetencie pri správe sieťových zariadení sú definované podľa nasledovnej tabuľky:

Sieť	Typ zariadenia	Konfigurácia	Prevádzka
Intranet	Firewall, router, switch	IT oddelenie	Dodávatelia
Extranet	Firewall, linky	IT oddelenie+dodávatelia	Dodávatelia
Internet	SaaS služby	Dodávatelia	Dodávatelia

Zamestnanci sú povinní dodržiavať nasledovné pravidlá zamerané na ochranu dôvernosti a integrity údajov prechádzajúcich cez verejné siete alebo cez bezdrôtové siete:

- Používať len šifrované komunikačné protokoly (https, sftp, a pod.)
- Informácie klasifikované ako Tajné a Prísne tajné vždy šifrovať dodatočne a heslo posielať iným kanálom ako šifrovaný obsah

Sieť je neustále monitorovaná podľa nasledujúcej tabuľky:

Typ zariadenia	Monitoring	Notifikácia
Firewall, router, switch	SIEM	IT oddelenie
Firewall, linky	Zabix	Dodávatelia
SaaS služby	SaaS monitoring	IT oddelenie

Za autentifikáciu systémov pripojených k sieti a obmedzenie pripojenia zodpovedá IT oddelenie, ktoré má k dispozícii nasledovné nástroje:

Typ zariadenia	Použitá technológia	Notifikácia
Firewall, router, switch	MAC address filtering	IT oddelenie
Koncové zariadenia	802.1x	IT oddelenie
Multifinkčné zariadenia	MAC address filtering	IT oddelenie

Zaregistrovanie nepovoleného zariadenia je vyhodnocovaná ako bezpečnostný incident.

HackMeBank definuje zodpovednosti a postupy pre správu sieťových zariadení nasledovne:
- centrálny manažment prístupov do aktívnych sieťových prvkov
- prístup je možný len z virtuálneho prostredia umiestneného v sieti banky, nie priamo zo zariadenia dodávateľa
- všetky prístupy sú logované
- prístup cez SSH na firewall má len dodávateľ, prístup cez tenkých / tučných klientov majú len zamestnanci banky

Dodatočné kontroly na ochranu dôvernosti a integrity údajov prechádzajúcich cez verejné siete alebo cez bezdrôtové siete:
- neustály monitoring siete pomocou IDS/IPS;
- zabezpečiť autentifikáciu systémov pripojených k sieti a obmedziť pripojenia;
- pravidelné školenia sieťových administrátorov v oblasti kybernetickej bezpečnosti.

A.13.1.3. Segregácia v sieťach

Obvod pre každú doménu je definovaný v IP pláne (v zodpovednosti IT oddelenia) a prístup medzi sieťovými doménami je riadený pomocou brány. Požiadavky na zmenu musia byť zadané cez štandardný požiadavkový systém a schválené vlastníkmi sieťových segmentov. Číslo požiadavky musí byť uvedené aj v pri firewallovom pravidle.

Príklad požiadavky je uvedený v nasledujúcej tabuľke:

Zdrojová IP adresa	Cieľová IP adresa	Port	Popis	Číslo incidentu
192.168.1.10	192.168.2.10	TCP 443	Prístup na intranetový portál	#123456

A.13.2. Prenos informácií

- pravidlá na ochranu pred škodlivým softvérom, ktorý sa môže prenášať prostredníctvom elektronickej komunikácie;
- pravidlá prijateľného používania komunikačných prostriedkov;
- explicitné pravidlá zakazujúce zamestnancom kompromitovať organizáciu (napr. ohováraním, obťažovaním, vydávaním sa za identitu, preposielaním reťazových listov, neoprávneným nákupom);
- šifrovať informácie (ak je to potrebné);
- pravidlá uchovávania a likvidácie obchodnej korešpondencie;
- nenechávať správy obsahujúce dôverné informácie na odkazovačoch, pretože ich môžu prehrať neoprávnené osoby;
- nenechávať citlivé informácie v tlačiarňach alebo faxoch;

- pracovníci upozornení, aby neviedli dôverné rozhovory na verejných miestach alebo prostredníctvom nezabezpečených komunikačných kanálov.

A.13.2.1. Zásady a postupy prenosu informácií

Pravidlá pre zamestnancov HackMeBank na ochranu pred škodlivým softvérom, ktorý sa môže prenášať prostredníctvom elektronickej komunikácie:

- Používať silné heslá a aktualizovať ich pravidelne.
- Neotvárajť prílohy e-mailov od neznámych zdrojov.
- Pravidelne aktualizovať antivírusový systém.
- Používať firewally pre zabezpečenie svojho siete pri homeoffice.
- Zálohovať svoje dáta a informácie a ukladať ich na firemných serveroch.
- Nepoužívať nebezpečné webové stránky a nezdieľajte nebezpečné súbory.
- Uistiť sa, že všetky firemné zariadenia (smartfóny, počítače atď.) sú zabezpečené a každé podozrivé správanie hlásiť IT oddeleniu.
- Používať len bezpečné metódy prenosu dát (napríklad šifrovanie, VPN atď.).

Zamestnancom je zakázané akým-koľvek spôsobom kompromitovať organizáciu napr.

- ohováraním,
- obťažovaním,
- vydávaním sa za identitu,
- preposielaním reťazových listov,
- neoprávneným nákupom;

Zamestnanci sú povinní šifrovať informácie klasifikované ako Prísne tajné dodatočným šifrovaním a heslo poslať nezávislým kanálom.

Zamestnanci HackMeBank sú povinní dodržiavať pravidlá uchovávania a likvidácie obchodnej korešpondencie (MIFID). V prípade nejasností sú povinní kontaktovať oddelenie Compliance.

Zamestancom je ďalej zakázané:
- nechávať správy obsahujúce dôverné informácie na odkazovačoch, pretože ich môžu prehrať neoprávnené osoby;
- nechávať citlivé informácie v tlačiarňach alebo faxoch;
- visť dôverné rozhovory na verejných miestach alebo prostredníctvom nezabezpečených komunikačných kanálov.

A.13.2.3. Elektronické zasielanie správ

Zamestnanci by mali používať v emailovej komunikácii nasledujúce pravidlá:

- Používať silné heslá a aktualizovať ich pravidelne.
- Vyhýbať sa sťahovaniu emailových príloh z neznámeho zdroja.
- Používať vyhradené e-maily pre komunikáciu s nedôveryhodnými zdrojmi (napr. hello@hackmebank.sk)
- Používať softvér na detekciu škodlivého softvéru na ochranu proti malware.
- Neotvárať e-maily alebo prílohy od neznámych osob.

- Nezabudnúť si prečítať podmienky a licenčné ujednania pred sťahovaním alebo inštaláciou softvéru.
- Zdieľať svoje e-maily len so spoľahlivými zdrojmi.
- Pravidelne zálohovať svoje e-maily.

A.14 System acquisition, development and maintenance

A.14.1. Bezpečnostné požiadavky informačných systémov

A.14.1.1. Analýza a špecifikácia požiadaviek na informačnú bezpečnosť

Za definovanie, aktualizáciu a vyhodnocovanie implementácie bezpečnostných požiadaviek je zodpovedný security manažér.
Security manažér môže v niektorých prípadoch poveriť interné oddelenie k súčinnosti počas posudzovania bezpečnosti výberu novej technológie, napr. RFI, RFP.

A.14.1.3. Ochrana transakcií aplikačných služieb

Používanie elektronického podpisu v internej a externej komunikácii:

- Elektronický podpis by mal byť šifrovaný, aby bolo zabezpečené, že správa bude doručená len tomu, komu má byť doručená.
- Elektronický podpis by mal byť autentifikovaný napr. používaním autentifikovaného prístupu do aplikácií, aby bolo zaručené, že správa pochádza od toho, za koho sa vydáva.
- Správy s elektronickým podpisom by mali byť chránené pred poškodením alebo úpravami, napr. používaním internej emailovej služby.
- Správy s elektronickým podpisom by mali byť dostupné len pre povolené osoby.
- Elektronický podpis by mal byť používaný iba v prípade, že je to technicky možné.
- Pri používaní elektronického podpisu by sa mali dodržiavať všetky zákonné požiadavky.

Pre elektronický podpis v transakčných systémoch platia nasledovné pravidlá:

- Elektronický podpis musí byť unikátny pre používateľa a musí byť vždy autentický a spoľahlivý.
- Elektronický podpis musí byť vytvorený pomocou certifikovaných technológií, ktoré sú schválené security manažérom.
- Elektronický podpis musí byť vždy asociovaný s jedinečným menom alebo identifikátorom používateľa.
- Elektronický podpis musí byť chránený pred neoprávneným prístupom alebo zneužitím.
- Elektronický podpis musí byť vždy zdokumentovaný a uložený v bezpečnom prostredí, aby sa zamedzilo jeho strateniu alebo poškodeniu.
- Elektronický podpis musí byť vždy platný a schválený internou službou na verifikáciu podpisu.
- Ďalšie podmienky používania elektronického podpisu musia byť určené security manažérom.

A.14.2. Bezpečnosť vo vývojových a podporných procesoch

A.14.2.1. Bezpečná vývojová politika

Bezpečnosť vývojového prostredia: HackMeBank má vyvinutý postup na kontrolu bezpečnosti vývojového prostredia, vrátane kontroly na úrovni prístupu, prevencie proti malware a vytvorenie auditu bezpečnosti. Prostredia sú navzájom oddelené, do produkcie developeri nemajú prístup.

Pokyny pre bezpečné kódovanie: HackMeBank má vyvinutý postup na zabezpečenie bezpečného kódovania, vrátane kontrol prístupu, prevencie proti malware a iných bezpečnostných opatrení. Počas deploymentu každej novej verzie prebieha automatizované skenovanie pomocou statickej analýzy kódu (SonarCube). Ku každému zisteniu sa vyjadruje developer (autor kódu) a nezapracované mitigácie musia byť akceptované manažérom kybernetickej bezpečnosti.

Bezpečnosť kontrolných bodov v rámci míľnikov projektu: HackMeBank má vyvinutý postup na kontrolu bezpečnosti pre každý míľnik projektu, vrátane kontroly prístupu, prevencie proti malware a vytvorenie auditu bezpečnosti. Počas míľnikov prebieha interný penetračný test a zistenia sú analyzované a riešenia zapracované do najbližšieho releasu.

Bezpečnosť v správe verzií: HackMeBank má vyvinutý postup na kontrolu bezpečnosti správy verzií, vrátane kontroly prístupu, prevencie proti malware a vytvorenie auditu bezpečnosti.

A.14.2.2. Postupy riadenia zmeny systému

Autorizácia zmien je vykonaná správcami systému, ktorí schvaľujú a podpisujú návrhy na zmeny. Núdzové opatrenia sa uskutočňujú v prípade núdze na obnovenie systému do jeho predchádzajúceho stavu (BCM procesy).
Recenzie a testy sú vykonávané na všetky zmenové požiadavky, aby sa zabezpečilo, že zmeny nebudú mať negatívny vplyv na chod systém.
Kontrola verzií všetkých aktualizácií softvéru zahŕňa kontrolu kvality a porovnávanie s predchádzajúcimi verziami. Každá nová verzia je digitálne podpísaná manažérom kybernetickej bezpečnosti.
Audit všetkých zmien zahŕňa prehľad všetkých zmien, aby sa zabezpečilo, že sa zmeny nevykonávajú bez autorizácie. Aktualizovanie dokumentácie systému je dokončené po dokončení a aplikovaní zmeny.
Implementácia zmien sa uskutočňuje tak, aby nebolo narušenie obchodných procesov (podľa aktuálneho stavu BCM).

A. 14.2.5. Princípy bezpečného systémového inžinierstva

- Identifikácia rizík: Identifikácia rizík je dôležitým krokom pri vytváraní bezpečných systémov. V HackMeBank sa vykonáva analýza rizík týkajúcich sa bezpečnosti, aby sa mohli odstrániť potenciálne bezpečnostné hrozby.
- Vývoj bezpečnostných politík: Vytvorenie a implementácia bezpečnostných politík je dôležitou súčasťou bezpečnostného inžinierstva. Politiky sú vyvážené, aby sa dosiahla optimálna úroveň bezpečnosti.
- Kontrola dostupnosti: Dostupnosť systému je jedným z najdôležitejších aspektov bezpečnostného inžinierstva. V HackMeBank je zabezpečené, aby systém bol dostupný počas celého času prevádzky, aby sa minimalizovala úroveň rizík.
- Ochrana dát a informácií: Ochrana dát a informácií je nevyhnutná pre zabezpečenie bezpečnosti. V HackMeBank je zabezpečené, aby boli všetky dáta a informácie uložené a zdieľané v bezpečnom prostredí.
- Monitorovanie systému: Monitorovanie systému je nevyhnutné pre účinné riadenie bezpečnosti. V HackMeBank sa vykonáva pravidelné monitorovanie systému, aby sa zistili potenciálne slabé miesta a zabezpečila úroveň bezpečnosti.
- Poskytovanie zákazníckych služieb: Poskytovanie zákazníckych služieb je dôležitou súčasťou bezpečnostného inžinierstva. V HackMeBank je zabezpečené, aby boli zákazníckym službám poskytované potrebné informácie, aby sa zabezpečila účinná ochrana dát.

A. 14.2.6. Bezpečné vývojové prostredie

- Citlivosť spracovávaných, uchovávaných a prenášaných údajov: V neprodukčných prostrediach je zakázané spracovávať produkčné dáta.
- Platné predpisy – externé alebo interné politiky: V HackMeBank sú implementované politiky, ktoré sú v súlade s externými predpismi a reguláciami, ako napríklad GDPR, a sú prispôsobené potrebám organizácie. V prípade nejasností je k dispozícii rola data privacy officera, ktorá je zodpovedná za riešenie problémov a kontrolu súladu s reguláciami.
- Dôveryhodnosť zainteresovaného personálu: HackMeBank má vytvorené postupy na verifikáciu a kontrolu totožnosti personálu, ktorí pracujú s citlivými údajmi alebo pracujú s vývojovým prostredím. Postupy sú v kompetencii oddelenia ľudských zdrojov.
- Outsourcované činnosti: HackMeBank má vytvorené postupy pre preskúmanie a monitorovanie dodávateľov, ktorí majú prístup k vývojovému prostrediu, a pre riadenie ich činností v rámci tohto prostredia. Súčasťou zmluvy s dodávateľom je aj príloha zameraná na zoznam bezpečnostných požiadaviek. Dodávatelia sú povinní riadiť sa podľa požiadaviek v prílohe.
- Kontrola prístupu do vývojového prostredia: HackMeBank má vytvorené postupy na identifikáciu, autentifikáciu a autorizáciu prístupu do vývojového prostredia. Do neprodukčných prostredí sú developeri povinný používať neprodukčné doménové účty. Akékoľvek výnimky sú developeri povinný konzultovať s manažérom informačnej bezpečnosti.
- Audit systému a zabezpečenia: HackMeBank má vytvorené postupy pre pravidelné audity systému a zabezpečenia, aby sa zabezpečilo, že všetky bezpečnostné požiadavky sú dodržiavané. Zistenia z auditov sú predložené aplikačnému vlastníkovi

systému, ktorý je povinný zapracovať navrhované riešenia do návrhu ďalšej verzie aplikácie.
- Zabezpečenie proti útokom: HackMeBank má vytvorené postupy na detekciu a odstránenie útokov a zabezpečenie proti útokom. Tieto systémy sú súčasťou architektúry informačnej bezpečnosti, všetky zmeny súvisiace s útokmi je preto potrebné konzultovať s architektúrou informačnej bezpečnosti.
- Riadenie rizík: HackMeBank má vytvorené postupy na identifikáciu, hodnotenie a riadenie rizík súvisiacich s vývojovým prostredím. Identifikácia rizík je povinnou súčasťou projektovej metodiky, za ktorú je zodpovedné oddelenie riadenia projektov.

A. 14.2.8. Testovanie bezpečnosti systému
Testovanie bezpečnosti je povinnou súčasťou každej zmenovej požiadavky. Pred vydaním novej verzie softvéru je potrebná príprava rizikovej analýzy, za ktorú je zodpovedné oddelenie informačnej bezpečnosti.
Všetky identifikované riziká je potrebné od konzultovať s developerským tímom a navrhované migrácie je potrebné zapracovať do existujúceho riešenia.
Rizika, na ktoré nie je možné implementovať mitigačné opatrenie, je potrebné akceptovať útvarom, ktorý je zadané riziko zodpovedný.

A. 14.2.9. Akceptačné testovanie systému
Za akceptačného testovania systémov je zodpovedný vlastník systému. Počas akceptačného testovania je preverená funkčnosť zmeny, ktorá bola predmetom dodávky.

A.14.3. Testovacie údaje
A. 14.3.1. Ochrana testovacích údajov
V HackMeBank je zakázané akékoľvek testovanie na produkčných dátach. Nejasnosti musia byť vždy od konzultované s Data Privacy offiserom.

A.16 Information security incident management
A.16.1. Riadenie incidentov a vylepšení informačnej bezpečnosti
A. 16.1.1. Zodpovednosti a postupy
V HackMeBank existujú procesy na účinnú a včasnú reakciu na incidenty informačnej bezpečnosti. Zúčastnené strany sú povinné dodržiavať nasledujúce postupy.

Plánovanie a príprava reakcie na incidenty:
- vytvorenie postupu na riadenie incidentov a bezpečnostných udalostí;
- vytvorenie bezpečnostného tímu;
- získanie právnych súhlasov;
- získanie informácií o incidente;
- získanie potrebných zdrojov na reagovanie na incident;
- identifikovanie dôležitých údajov a prístupov;
- definovanie postupov pre vyšetrovanie incidentov.

Zodpovednosť: Aplikačný vlastník.

Monitorovanie, zisťovanie, analyzovanie a hlásenie bezpečnostných udalostí a incidentov:
- zavedenie systému monitorovania a zisťovania bezpečnostných udalostí;
- vytvorenie postupu pre identifikáciu potenciálnych incidentov;
- vytvorenie postupu pre správu a analyzovanie incidentov;
- vytvorenie postupu pre odosielanie správ o incidentoch;
- vytvorenie postupu pre prevenciu podobných incidentov v budúcnosti.

Zodpovednosť: IT oddelenie

Správa incidentov pri logovaní:
- vytvorenie postupu pre správu logovania;
- vytvorenie postupu pre správu užívateľských účtov;
- zavedenie systému pre umožnenie sledovania všetkých prístupov k systému;
- vytvorenie postupu pre správu a analyzovanie logov;
- vytvorenie postupu pre identifikovanie potenciálnych incidentov a následných opatrení;
- zavedenie systému pre sledovanie všetkých úprav súborov a zmien v systéme.

Zodpovednosť: IT oddelenie

Eskalácia incidentov a zotavenie sa z incidentu:
- vytvorenie postupu pre eskaláciu incidentov;
- zavedenie systému pre identifikovanie vyšších rizík;
- vytvorenie postupu pre správu a analyzovanie incidentov;
- vytvorenie postupu pre odstránenie príčin incidentu;
- vytvorenie postupu pre obnovenie systému;
- vytvorenie postupu pre zotavenie sa z incidentu.

Zodpovednosť: Aplikačný vlastník

A.16.1.2. Hlásenie udalostí informačnej bezpečnosti

Za bezpečnostnú udalosť, ktorú je potrebné nahlásiť, je považované:
- bezpečnostná kontrola, ktorá nie je účinná;
- ľudské chyby;
- vírus zistený v systéme;
- porušenie fyzickej bezpečnosti vedúce ku krádeži;
- odhalenie hesiel;
- hardvér alebo softvér, ktorý nefunguje správne;
- nekontrolované zmeny systému;
- neoprávnený prístup k systémom;
- nedodržiavanie zákonných požiadaviek alebo postupov...

Všetky udalosti informačnej bezpečnosti je povinné hlásiť na emailovú adresu incident@hackeme.bank .

A.16.1.3. Hlásenie slabých stránok informačnej bezpečnosti

Mechanizmus reportovania správ zahŕňa jednoduchý formulár na webovej stránke, ktorý sú používatelia povinní vyplniť, aby nahlásili slabú stránku. Formulár požaduje, aby používatelia uviedli podrobnosti slabého miesta, ako je napríklad typ údajov ktorý je ohrozený, ako aj časový rámec, v ktorom sa objavila slabina. Je potrebné uviesť odkaz (adresu URL). IT

oddelenie je povinné po preverení takejto stránky zabezpečiť automatizované kontrolné procesy s cieľom znížiť prístup ostatných používateľov na dané stránky (napríklad blokovaním na bránach).

A.16.1.5. Reakcia na incidenty informačnej bezpečnosti

V HackMeBank platí nasledujúci postup na reagovanie na incidenty informačnej bezpečnosti:
1. Vytvoriť zdokumentovaný postup pre riešenie incidentov informačnej bezpečnosti, ktorý by mal zahŕňať:
- kroky pre vyhodnotenie incidentu;
- postupy pre zhromažďovanie dôkazov;
- postupy pre analýzu incidentu;
- postupy pre eskaláciu do vyšších štruktúr;
- postupy pre komunikáciu so všetkými zainteresovanými stranami;
- postupy pre identifikáciu slabých stránok, ktoré vedú k incidentu;
- postupy pre zaznamenávanie incidentu;
- postupy pre uzatváranie incidentu.
2. Uistiť sa, že všetci pracovníci sú oboznámení s postupmi pre riešenie incidentov informačnej bezpečnosti.
3. Monitorovať aktivity súvisiace s informačnou bezpečnosťou a identifikovať možné problémy a incidenty.
4. Vyhodnotiť incident podľa poskytnutých postupov a zaznamenať ho.
5. Ak je to potrebné, eskalovať incident na vyššie úrovne.
6. Zhromaždiť dôkazy a vykonať analýzu.
7. Komunikovať s všetkými stranami, ktoré potrebujú vedieť o incidente.
8. Identifikovať slabé stránky, ktoré vedú k incidentu, a vysporiadať sa s nimi.
9. Zaznamenať incident pre účely neskoršieho auditu a uzatvoriť ho.

A.16.1.7. Zhromažďovanie dôkazov

HackMeBank by mala zhromažďovať a uchovávať informácie, ktoré môžu slúžiť ako dôkaz podľa zavedených postupov. Vo väčšine prípadov nie je jasné, či určitý incident skončí na súde alebo nie. Organizácia by mala zhromažďovať informácie, ktoré môžu slúžiť ako dôkaz pre každý incident bezpečnosti informácií.
HackMeBank má nasledujúce postupy na nakladanie so zhromaždenými dôkazmi.

1. Každý incident bezpečnosti informácií by sa mal zaznamenať do záznamov, v ktorých by sa uchovávali dôkazy.
2. Všetky zhromaždené dôkazy by sa mali uchovávať v bezpečnom a zabezpečenom prostredí.
3. Každý dôkaz by mal byť označený dátumom a časom, keď sa zhromaždil.
4. Všetky dôkazy by mali byť uchovávané po dobu minimálne 5 rokov.
5. Všetky dôkazy by mali byť dostupné pre príslušné osoby, ktoré ich budú potrebovať na prešetrovanie incidentu.
6. Všetky dôkazy by mali byť systematicky monitorované a kontrolované, aby sa zabezpečilo, že sú vždy v bezpečí.

7. V prípade potreby by mali byť dôkazy vymazané alebo presunuté do iného bezpečného prostredia.

Zoznam obrázkov

Prílohy

- ISO 27001

INTERNATIONAL STANDARD

ISO/IEC 27001

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC FDIS 27001:2013(E)