STRATEGIE INFORMAČNÍ BEZPEČNOSTI

Obsah

Předmluva

Jako banka a pojišťovna orientovaná na budoucnost je KBC oddaná svým zákazníkům a plně přijímá digitální inovace, aby optimalizovala a diverzifikovala své služby. Na této cestě se řízení rizik a bezpečnosti stalo ještě důležitější prioritou pro všechny entity ve skupině. V dnešním světě organizované hackerské skupiny neustále testují obranu společností, hledají slabiny, které mohou využít ke krádeži dat nebo kompromitaci interních systémů. KBC je odhodlána zůstat v tomto závodě napřed, kombinovat sílu mnoha proaktivních bezpečnostních kontrol s detekčními a reakčními schopnostmi dostatečně silnými na to, aby zastavily všechny útoky dlouho předtím, než by mohly způsobit jakoukoli škodu.

„Strategie informační bezpečnosti skupiny KBC“ stanovuje základní principy a stavební bloky pro dosažení tohoto cíle. Dokument ilustruje naši komplexní vizi řízení informační bezpečnosti a způsob, jakým všechny obchodní entity a IT spolupracují, aby naplnily tento závazek a chránily data našich zákazníků.

Christine Van Rijsseghem
Chief Risk Officer, KBC Group

Erik Luts
Chief Innovation Officer, KBC Group

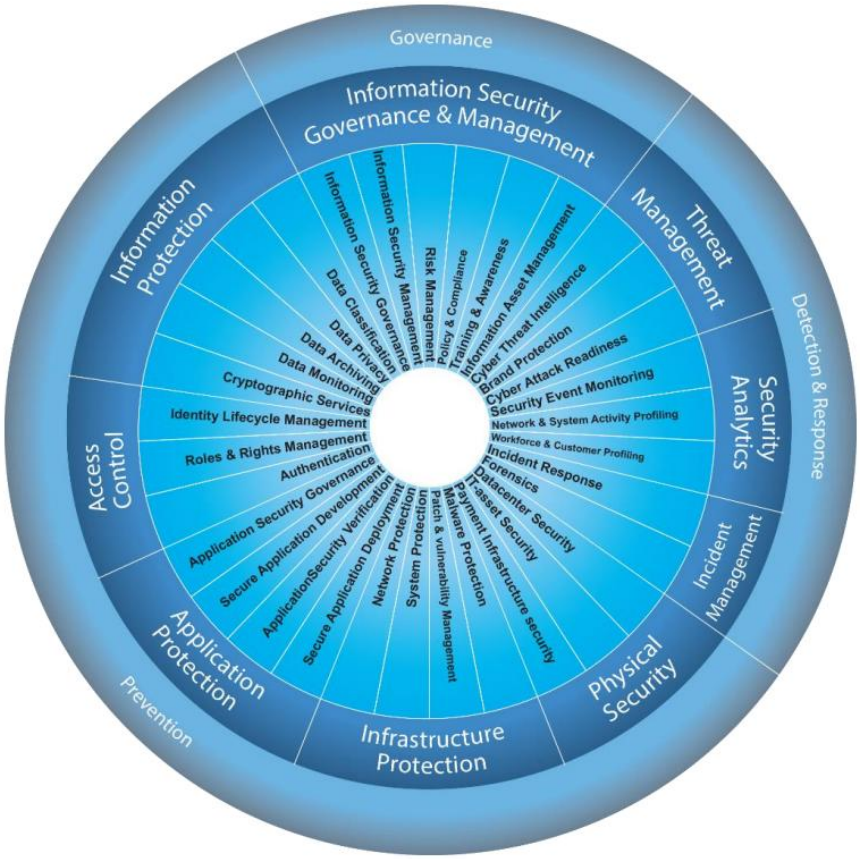
Úvod

Dnešní prostředí hrozeb neustále připomíná organizacím, že bezpečnostní incidenty nejsou možností, ale jistotou. Nejde o to, zda organizace zažije bezpečnostní incident, ale kdy. To znamená, že je zásadní, aby každá organizace měla zavedený robustní program informační bezpečnosti, který je sladěn s její strategií informační bezpečnosti.

S tímto vědomím a za účelem ochrany svých zákazníků a akcionářů považuje skupina KBC svou strategii informační bezpečnosti za klíčový prvek své správy informační bezpečnosti. Požadavkem, aby všechny její entity vypracovaly bezpečnostní strategii s jasnými cíli a metrikami, skupina KBC proaktivně řeší negativní dopady bezpečnostních incidentů, vyhýbá se zbytečným nákladům a ztrátám, a nakonec poskytuje konkurenční výhodu v okamžiku rozhodování při výběru produktů, služeb a obchodních partnerů.

Toho je dosaženo prostřednictvím bezpečnostních kontrol, které skupina KBC neustále zavádí a udržuje. Jedná se o dynamický, živý soubor bezpečnostních opatření založený na nejlepších prvcích norem ISO, rámce kybernetické bezpečnosti NIST a vlastních zkušenostech KBC s informační bezpečností. Současně tato opatření stanovují závazné právní a regulační požadavky, které skupina KBC dodržuje, včetně obecného nařízení o ochraně osobních údajů (GDPR) a právních aktů Evropské centrální banky (ECB).

Obrázek 1 – Informační strategický rámec skupiny KBC



Klíčové kontroly informační bezpečnosti skupiny KBC – přehled

Skupina KBC definovala svůj „vesmír“ informační bezpečnosti na základě vysokých standardů. Je postaven na devíti schopnostech, rozdělených do 33 dílčích schopností („klíčových kontrol“). Tyto klíčové kontroly zahrnují oblasti od správy, prevence, detekce až po reakci a pokrývají celý životní cyklus informační bezpečnosti. Klíčové kontroly jsou:

- **Řízení informační bezpečnosti (Information Security Governance)** – Zahrnuje zavedené vedení, principy, procesy a organizační struktury, které řídí realizaci správy informační bezpečnosti ve skupině KBC.
- **Správa informační bezpečnosti (Information Security Management)** – Týká se všech požadavků, jako jsou procesy, organizační struktury, kultura, rámce, stavební bloky a zdroje (informace, řešení, lidé, dovednosti atd.), které skupina KBC uplatňuje každodenně v souladu se směrem stanoveným prostřednictvím procesu řízení.
- **Řízení rizik (Risk Management)** – Skupina KBC má zavedený účinný systém řízení rizik informační bezpečnosti, který propojuje ochotu podstupovat riziko s obchodní strategií a definuje relevantní kontroly pro celou organizaci. Účinnost těchto kontrol založených na riziku se měří, aby skupina KBC mohla zaručit svým zákazníkům (a společnosti obecně), vrcholovému vedení a externím subjektům (např. regulátorům), že rizika informační bezpečnosti jsou řádně řízena.
- **Politika a shoda (Policy & Compliance)** – Komplexní rámec politik skupiny KBC má za cíl vytvářet a přijímat správné politiky a standardy a zahrnuje procesy pro měření znalostí a dodržování těchto politik a standardů. Politiky a standardy obsahují povinné požadavky, kontroly, postupy, role a odpovědnosti nebo specifikace v souladu s osvědčenými postupy informační bezpečnosti.
- **Školení a povědomí (Training & Awareness)** – Skupina KBC považuje komplexní program školení a zvyšování povědomí za klíčový pro vytvoření povědomí o rizicích spojených s informační bezpečností a o krocích, které organizace podniká k boji proti těmto rizikům, napříč celou organizací – od představenstva a vrcholového vedení až po všechny zaměstnance, partnery a třetí strany. Za tímto účelem jsou programy školení a povědomí přizpůsobeny cílovým skupinám, aktualizovány v souladu s prostředím hrozeb a jejich účinnost je neustále měřena. Kromě toho skupina KBC přispívá ke zvyšování povědomí o bezpečnosti mezi svými zákazníky a ve společnosti jako celku – například prostřednictvím každoročních národních kampaní kybernetické bezpečnosti organizovaných skupinou KBC.
- **Správa informačních aktiv (Information Asset Management)** – Informační aktiva, jak v digitální, tak fyzické podobě, jsou identifikována a je vytvořen a udržován jejich inventář.
- **Klasifikace dat (Data Classification)** – Klasifikace dat ve skupině KBC je založena na povaze dat (např. osobní identifikovatelné údaje, finanční informace atd.) a na stupni citlivosti dat a dopadu na společnost, pokud by tato data byla zveřejněna, změněna,

zničena, ztracena, přenesena nebo zpracována nelegitimně. Systém klasifikace skupiny KBC je jednoduchý na pochopení, používání a jednotné uplatňování v celé organizaci.

- **Ochrana soukromí dat (Data Privacy)** – Pro skupinu KBC je velmi důležité porozumět požadavkům a postupům ochrany soukromí při shromažďování, ukládání, používání, sdílení a přenosu osobních údajů. Z tohoto důvodu a za účelem ochrany osobních údajů před krádežemi a podvody jsou tyto informace ukládány bezpečným způsobem, který je chrání před neoprávněným přístupem.
- **Archivace dat (Data Archiving)** – Archivace dat se týká procesu správné archivace citlivých informací ve skupině KBC: decentralizovaně na úrovni koncového bodu nebo serveru, centralizovaně v kolaborativním prostoru, v dedikovaném archivačním řešení (pro „staré“ informace, které je třeba uchovat po určitou dobu) nebo v záložním systému. Každá z těchto oblastí úložiště je chráněna v souladu s citlivostí informací.
- **Monitoring dat (Data Monitoring)** – Monitoring dat – nebo obecněji monitorování a prevence úniku dat – je ve skupině KBC implementováno za účelem ověření, zda jsou citlivé informace bezpečně uloženy, odesílány a používány. Skupina KBC má k dispozici několik nástrojů nejen pro prevenci ztráty dat, ale také pro monitorování dat v klidu, při používání nebo při přenosu. S příchodem chytrých telefonů, tabletů a osobních notebooků do podnikových sítí se monitorování a prevence úniku dat rozšiřuje i mimo hranice organizace KBC, aby se zabránilo neúmyslným nebo úmyslným únikům dat.
- **Kryptografické služby (Cryptographic Services)** – Kromě požadavku na používání kryptografie k ochraně informací na základě jejich citlivosti a vystavení skupina KBC také uplatňuje kryptografické techniky tam, kde je to potřeba, včetně šifrování, správy certifikátů, bezpečných postupů správy klíčů a kontrol integrity. Skupina KBC také definuje, kdy a jak jsou informace šifrovány, aby byla zajištěna účinná a efektivní ochrana.
- **Autentizace (Authentication)** – Aby bylo možné určit, zda je někdo skutečně tím, za koho se vydává, má skupina KBC zavedeno několik bezpečnostních kontrol. Jedním z příkladů je použití vícefaktorové autentizace, která se používá ke zvýšení jistoty, že uživatel je skutečně tím, za koho se vydává, a k zabránění neoprávněné manipulace s přihlašovacími údaji.
- **Správa identit (Identity Management)** – Správa identit ve skupině KBC zahrnuje správu digitálních identit a přihlašovacích údajů uživatelů po celou dobu jejich působení v systémech nebo aplikacích skupiny KBC. Správa životního cyklu identit se týká také obecných účtů a strojových účtů, které rovněž vyžadují vlastníka odpovědného za ně.
- **Správa rolí a oprávnění (Roles & Rights Management)** – Skupina KBC má zavedený proces správy oprávnění, který určuje, jaké akce může nebo nemůže ověřená identita provádět v rámci aplikace. Aby se omezilo riziko nežádoucích nebo náhodných změn, jsou práva přiřazená identitě sladěna s obchodní potřebou, ale zároveň podporují princip minimálních oprávnění a oddělení povinností.

- **Řízení bezpečnosti aplikací (Application Security Governance)** – Řízení bezpečnosti aplikací ve skupině KBC zahrnuje procesy a činnosti, prostřednictvím kterých jsou dosaženy celkové cíle a záměry vývoje softwaru.
- **Bezpečný vývoj aplikací (Secure Application Development)** – Skupina KBC definuje cíle a vytváří software v rámci vývojových projektů. Obecně to zahrnuje řízení produktů, provádění hodnocení hrozeb, definování bezpečnostních požadavků a jejich shromažďování, specifikaci bezpečné architektury na vysoké úrovni, detailní návrh a implementaci.
- **Ověřování bezpečnosti aplikací (Application Security Verification)** – Pro ověřování bezpečnosti aplikací skupina KBC kontroluje a testuje artefakty vytvořené během procesu vývoje softwaru. To obvykle zahrnuje práci v oblasti zajištění kvality, jako je testování bezpečnosti, ale také další kontroly návrhu a implementace.
- **Bezpečné nasazení aplikací (Secure Application Deployment)** – To zahrnuje procesy a činnosti, které skupina KBC provádí za účelem správy softwarových verzí, které byly vytvořeny. Může to zahrnovat dodávání produktů koncovým uživatelům, nasazování produktů na interní nebo externí hostitele a běžný provoz softwaru v prostředí běhu, jako je zpevňování prostředí a správa problémů.
- **Ochrana sítě (Network Protection)** – Ochrana sítě skupiny KBC je založena na zásadách bezpečnosti sítě a souvisejících standardech, aby se zabránilo neoprávněnému přístupu, zneužití, modifikaci nebo odmítnutí počítačových sítí a síťově dostupných zdrojů. Ochrana sítě zahrnuje jak interní, tak externí sítě a síťové zóny, které je propojují.
- **Ochrana systémů (System Protection)** – Aby se snížilo riziko kompromitace systémů, ochrana systémů ve skupině KBC zpevňuje systémy na základě jejich vystavení a citlivosti. Ověření základních konfigurací ochrany systémů poskytuje jistotu o aktuální úrovni zabezpečení. Bezpečnost koncových počítačů nebo mobilních zařízení vyžaduje zvláštní pozornost, protože tato zařízení jsou také vystavena kybernetickým hrozbám: ve mnoha případech jsou koncová zařízení vstupním bodem pro hackery.
- **Správa záplat a zranitelností (Patch & Vulnerability Management)** – Skupina KBC má zavedené procesy správy záplat a zranitelností, aby zabránila zneužití zranitelností existujících v informačních systémech. Ne všechny zranitelnosti mají dostupné záplaty; proto si správci systémů musí být vědomi nejen příslušných zranitelností a dostupných záplat, ale také jiných metod nápravy, které omezují vystavení systémů zranitelnostem.
- **Ochrana proti malwaru (Malware Protection)** – Infrastruktura skupiny KBC je chráněna proti malwaru. Tato ochrana je založena na vrstveném přístupu využívajícím jak kontroly založené na signaturách, tak na chování, s funkcemi, jako je detekce, prevence a obnova. Kromě toho skupina KBC denně podporuje vhodné povědomí uživatelů.
- **Bezpečnost datových center (Data Centre Security)** – Všechna datová centra a technologické místnosti obsahující IT vybavení skupiny KBC jsou fyzicky chráněna před neoprávněným přístupem a environmentálními riziky prostřednictvím kombinace přístupových kontrol a několika bezpečnostních opatření, která jsou pravidelně

přezkoumávána a aktualizována. Skupina KBC také zavedla metodologii 2x2 datových center a provádí časté testy obnovy po havárii.

- **Bezpečnost IT aktiv (IT Asset Security)** – Hodnotná IT aktiva umístěná na pracovištích skupiny KBC jsou chráněna před ztrátou, krádeží a zničením.
- **Bezpečnost platební infrastruktury (Payment Infrastructure Security)** – Napříč skupinou KBC jsou implementována vhodná fyzická a informační bezpečnostní opatření na ochranu jejích aktiv a citlivých platebních údajů zákazníků. Tato opatření se zaměřují jak na bezpečnost fyzických aktiv, tak na ICT systémy používané k poskytování platebních služeb.
- **Reakce na incidenty (Incident Response)** – Skupina KBC sleduje, reaguje, měří a shromažďuje metriky bezpečnostních incidentů napříč celou organizací. To zahrnuje plánování, koordinaci a provádění všech vhodných strategií a opatření pro zmírnění a obnovu. Pro zvýšení účinnosti je reakce na incidenty sladěna s obchodními cíli, regulačními povinnostmi a celkovou kulturou.
- **Forenzní analýza (Forensics)** – Skupina KBC zkoumá informační systémy forenzně robustním způsobem, aby identifikovala hlavní příčinu bezpečnostních incidentů, což umožňuje odhalení podrobností týkajících se typů útoků, metodologií a chování. Tyto informace lze následně použít na jiné kontroly k detekci a prevenci podobných událostí v budoucnu.
- **Monitorování bezpečnostních událostí (Security Event Monitoring)** – Skupina KBC shromažďuje a analyzuje bezpečnostní události, aby si udržela přehled o všech aspektech své informační bezpečnosti. To zahrnuje lidi, procesy a technologie, které neustále hodnotí úroveň viditelnosti poskytovanou shromážděnými daty, aby proaktivně identifikovaly mezery v pokrytí, příležitosti ke zlepšení zaznamenávání dat a optimalizovaly technologie používané k generování, shromažďování a korelaci dat událostí.
- **Profilování aktivity sítě a systému (Network and System Activity Profiling)** – Skupina KBC definuje normální aktivitu v rámci svých sítí a systémů; proto aktivita sítě nebo systému, která se odchyluje od této očekávané aktivity (anomálie), může naznačovat potenciální kybernetický útok. Jelikož skupina KBC proaktivně shromažďuje informace související s anomáliemi sítě, podrobné informace o chování malwaru, vektorech infekce, metodách útoku, změnách operačního systému (OS), komunikačních protokolech, interakci s infrastrukturou botnetů a dalších údajích relevantních pro způsob, jakým kyberzločinci operují, tato schopnost se vyvíjí v prediktivní systém schopný poskytovat data, která lze použít k předcházení kybernetickým útokům.
- **Profilování chování pracovníků a zákazníků (Workforce and Customer Behaviour Profiling)** – Profilování chování pracovníků a zákazníků umožňuje skupině KBC detekovat kybernetické útoky definováním normálního chování lidí a hledáním odchylek od tohoto očekávaného chování.
- **Zpravodajství o kybernetických hrozbách (Cyber Threat Intelligence)** – Skupina KBC shromažďuje, koreluje a analyzuje informace z různých zdrojů týkající se nejnovějších

kybernetických útoků a využívá odvozené poznatky k detekci, prevenci a reakci na útoky. Skupina KBC neustále a aktivně sleduje vývoj kybernetické kriminality s cílem získat přehled o vyvíjejícím se způsobu útoků, jakož i o motivech a cílech pachatelů. Konečným cílem je včas předvídat a narušit obchodní model kyberzločinců.

- **Ochrana značky (Brand Protection)** – V oblasti kybernetické bezpečnosti spočívá ochrana značky v nepřetržitém monitorování internetových odkazů na skupinu KBC a její značky za účelem shromažďování relevantních informací, které by mohly ohrozit image organizace, její pověst nebo bezpečnost informačních systémů, včetně detekce podvodných webových stránek spojených s phishingem nebo malwarem.
- **Připravenost na kybernetické útoky (Cyber Attack Readiness)** – Skupina KBC podporuje přípravu na kybernetické útoky testováním reakce na možný kybernetický útok, aby posoudila připravenost a schopnosti reakce a poskytla realističtější obraz o připravenosti na kybernetickou bezpečnost. Jedním ze způsobů, jak se to provádí, jsou cvičení etického hackingu.

Organizace informační bezpečnosti skupiny KBC – Rámec řízení rizik, role a odpovědnosti

V rámci Rámce řízení operačních rizik skupiny KBC (ORMF), který stanovuje standardy pro efektivní a účinné řízení operačních rizik napříč skupinou KBC, je v celé organizaci zaveden model tří linií obrany.

- ***První linie obrany:*** Samotný obchod. Obchodní část je plně odpovědná za všechna rizika ve své oblasti činnosti a musí zajistit, aby byla zavedena účinná kontrolní opatření. Tím zajišťuje, že správné kontroly jsou prováděny správným způsobem, že sebehodnocení obchodní části je na dostatečně vysoké úrovni, že existuje odpovídající povědomí o riziku a že je rizikovým tématům přidělena dostatečná priorita/kapacita. Z hlediska informační bezpečnosti leží odpovědnost za první linii obrany na pracovnících informační bezpečnosti (Information Security Officers) a místních manažerech operačních rizik (Local Operational Risk Managers).

- ***Druhá linie obrany:*** Hlavním cílem druhé linie obrany je poskytovat přiměřenou jistotu skupinovému CRO a místním CROs. Jsou podporováni místními pracovníky pro rizika, kteří jsou odpovědní za implementaci ORMF v rámci své působnosti. Dále Centra kompetencí (CoC) v rámci skupinového řízení rizik, podporovaná různými dalšími odbornými funkcemi druhé linie, jsou odpovědná za definování skupinového ORMF a souvisejících skupinových standardů, sledování implementace, skupinové reportování operačních rizik a podpůrné skupinové nástroje. Součástí skupinového řízení rizik je jednotka Group Information Risk Management (IRM), která se zaměřuje na informační rizika, včetně informační bezpečnosti, rizik souvisejících s IT a řízení kontinuity podnikání na úrovni skupiny. Zahrnuje také tým KBC Group Cyber Expertise and Response Team (CERT).

- ***Třetí linie obrany:*** Interní audit. – Jako nezávislá třetí linie kontroly je interní audit odpovědný za kontrolu kvality stávajících obchodních procesů. Provádí audity založené na riziku i obecné audity, aby zajistil, že systém vnitřní kontroly a řízení rizik, včetně politiky rizik, je účinný a efektivní, a aby zajistil, že opatření a procesy jsou zavedeny a konzistentně uplatňovány v rámci skupiny, což zaručuje kontinuitu provozu. Z hlediska informační bezpečnosti poskytuje interní audit nezávislou přiměřenou jistotu o přiměřenosti a účinnosti kontrolního prostředí.

Spolupráce skupiny KBC s regulátory

Skupina KBC podléhá dohledu několika regulátorů, včetně Evropského orgánu pro bankovnictví (EBA), Evropské centrální banky (ECB) a národních regulátorů v zemích, kde skupina KBC působí.
Skupina KBC podává zprávy těmto regulátorům a spolupracuje s nimi na řešení rizik informační bezpečnosti a zveřejňuje veřejně dostupné zprávy na stránkách Risk reports (kbc.com).

Současné a budoucí iniciativy informační bezpečnosti skupiny KBC

Závazek skupiny KBC k informační bezpečnosti se odráží také v jejích vlastních iniciativách v oblasti informační bezpečnosti, které řeší současné a budoucí výzvy a rizika vyplývající ze stále větší závislosti na IT. Technologie se nejen vyvíjí ohromujícím tempem *(AI, Internet věcí, 5G),* ale prostředí hrozeb se také stává stále sofistikovanějším. Kromě toho se po celém světě zavádějí další vylepšení stávajících předpisů o informační bezpečnosti, přičemž nové předpisy vstupují v platnost a dohled regulátorů nad dodržováním informační bezpečnosti se neustále zvyšuje.

Na tomto pozadí skupina KBC neustále přezkoumává a přizpůsobuje své vlastní bezpečnostní nastavení, přičemž se zaměřuje mimo jiné (ale nikoli výlučně) na:

- ***Povědomí uživatelů (User Awareness)*** – Kromě zvýšení kampaní na zvyšování povědomí o kybernetické bezpečnosti ve skupině KBC se stále více zaměřuje na zlepšování dovedností zaměstnanců v oblasti informační bezpečnosti. To umožňuje zaměstnancům skupiny KBC získat hlubší znalosti o informační bezpečnosti, což vede k lepšímu dodržování zásad informační bezpečnosti, a zároveň rozvíjet silnou interní komunitu informační bezpečnosti ve skupině KBC.
- ***Monitorování klimatu informační bezpečnosti (Information Security Climate Monitoring)*** – Spolu s podporou povědomí uživatelů skupina KBC také sleduje klima informační bezpečnosti v organizaci. To znamená zkoumání individuálních vnímání hodnoty informační bezpečnosti na základě politik, postupů a praktik v pracovním prostředí. Za tímto účelem skupina KBC vyvíjí nové metodiky a nástroje pro identifikaci a zavádění opatření, která usnadňují dodržování politik a postupů zaměstnanci a zabraňují praktikám, které by mohly vést k bezpečnostním incidentům.
- ***Řešení cílených phishingových hrozeb (Tackling Targeted Phishing Threats)*** – Phishingové útoky patří mezi hlavní bezpečnostní hrozby pro organizace. Útočníci používají stále pokročilejší metody při provádění útoků, které jsou navíc prováděny s stále vyšší mírou personalizace. Vedle probíhajících komplexních programů zvyšování povědomí o informační bezpečnosti skupina KBC odpovídajícím způsobem vylepšuje mechanismy prevence úniku dat, zlepšuje procesy bezpečnostní analytiky (včetně prediktivní bezpečnosti) a dále rozšiřuje segmentaci sítě napříč organizací. Kromě toho

zůstává implementace vícefaktorové autentizace na každém zařízení a systému skupiny KBC nezbytností.

- ***Etický hacking (Ethical Hacking)*** – Etický hacking je provádění penetračního testování na základě souhlasu s cílem odhalit potenciální zranitelnosti a zlepšit bezpečnost informačního systému organizace. Skupina KBC energicky podporuje cvičení etického hackingu, protože pomáhají zmírnit možné bezpečnostní mezery, vedou k přijetí nových preventivních opatření proti útočníkům a zásadně zlepšují celý její bezpečnostní systém.
- ***Správa zranitelností (Vulnerability Management)*** – Skupina KBC považuje správu zranitelností za základní součást své strategie kybernetické bezpečnosti. S tímto vědomím se nejen zlepšují postupy týkající se identifikace, prevence, zmírňování a klasifikace zranitelností, ale také se do organizace integrují nové nástroje pro správu zranitelností, aby tyto zranitelnosti detekovaly a vyvinuly záplaty a/nebo nápravná opatření k jejich zmírnění.
- ***Bezpečnost cloudu (Cloud Security)*** – Skupina KBC ve spolupráci se svými partnery poskytujícími cloudové služby neustále přezkoumává bezpečnost cloudů, ve kterých působí. Šifrovací a autentizační metody, auditní záznamy a oddělení dat musí být vždy zajištěny, a to jak pro data v pohybu, tak pro data v klidu.
- ***Struktura řízení (Governance Structure)*** – Skupina KBC pravidelně přezkoumává své vlastní řízení, aby zajistila, že role, odpovědnosti a procesy související s informační bezpečností jsou koherentní a že provádění jejího rámce řízení informační bezpečnosti zůstává efektivní. Současně jsou politiky, standardy a pokyny týkající se informační bezpečnosti neustále přezkoumávány a v případě potřeby přizpůsobovány novým výzvám a rizikům, včetně dodržování předpisů. Další informace naleznete na stránkách Corporate Governance (kbc.com).
- ***Strojové učení (Machine Learning)*** – Strojové učení se vyvíjí jako prostředek k předvídání a reakci na aktivní útoky v reálném čase. Strojové učení se také používá k analýze vzorců hrozeb a k získání dalších poznatků o chování kybernetických delikventů, aby bylo možné podobným útokům v budoucnu zabránit a snížit dobu potřebnou pro řešení bezpečnostních incidentů odborníky na informační bezpečnost.
- ***Pojištění (Insurance)*** – Skupina KBC má zavedený komplexní pojistný program, který zmírňuje možné finanční dopady kybernetické události.

Zdroje

European Banking Authority (www.eba.europa.eu)

European Central Bank (www.ecb.europa.eu)

Financial Services and Markets Authority (www.fsma.be)

General Data Protection Regulation (www.eur-lex.europa.eu)

International Organization for Standardization (www.iso.org)

KBC Group (www.kbc.com)

National Bank of Belgium (www.nbb.be)

Poznámka: Text je překladem z originálního dokumentu KBC "Information Security Strategy".