KATALÓG SLUŽIEB 2024

NAKIB

PORADENSKÉ SLUŽBY

NÁRODNÁ AKADÉMIA PRE KYBERNETICKÚ
A INFORMAČNÚ BEZPEČNOSŤ

NAKIB.SK

NAKIB

PORADENSKÉ SLUŽBY

Implementácia Kyber Security podľa ZoKB 69/2018

Implementácia Kyber Security podľa NIS2

Implementácia ISO 9001

Implementácia ISO 27001

Implementácia ISO 27005

Implementácia ISO 20000

Implementácia IEC 62443

Implementácia Biznis kontinuity (BCM)

Implementácia požiadaviek GDPR

Implementácia požiadaviek TISAX®

Implementácia požiadaviek DORA

Poskytovanie Vulnerability Manažmentu

Vykonávanie PEN Testov

Napojenie na SIEM system

Zabezpečenie Cloudových služieb

NAKIB.SK

PORADENSTVO A POSKYTOVANIE SLUŽIEB V OBLASTI KYBER SECURITY PODĽA ZOKB A JEDNOTLIVÝCH VYHLÁŠOK

Čo je?

Zákon o kybernetickej bezpečnosti (ZoKB) č. 69/2018 Z. z. definuje právne a technické požiadavky na kybernetickú bezpečnosť prevádzkovateľov základných služieb a orgánov verejnej moci. Cieľom je chrániť informačné systémy a siete pred kybernetickými hrozbami a incidentmi.

Prečo?

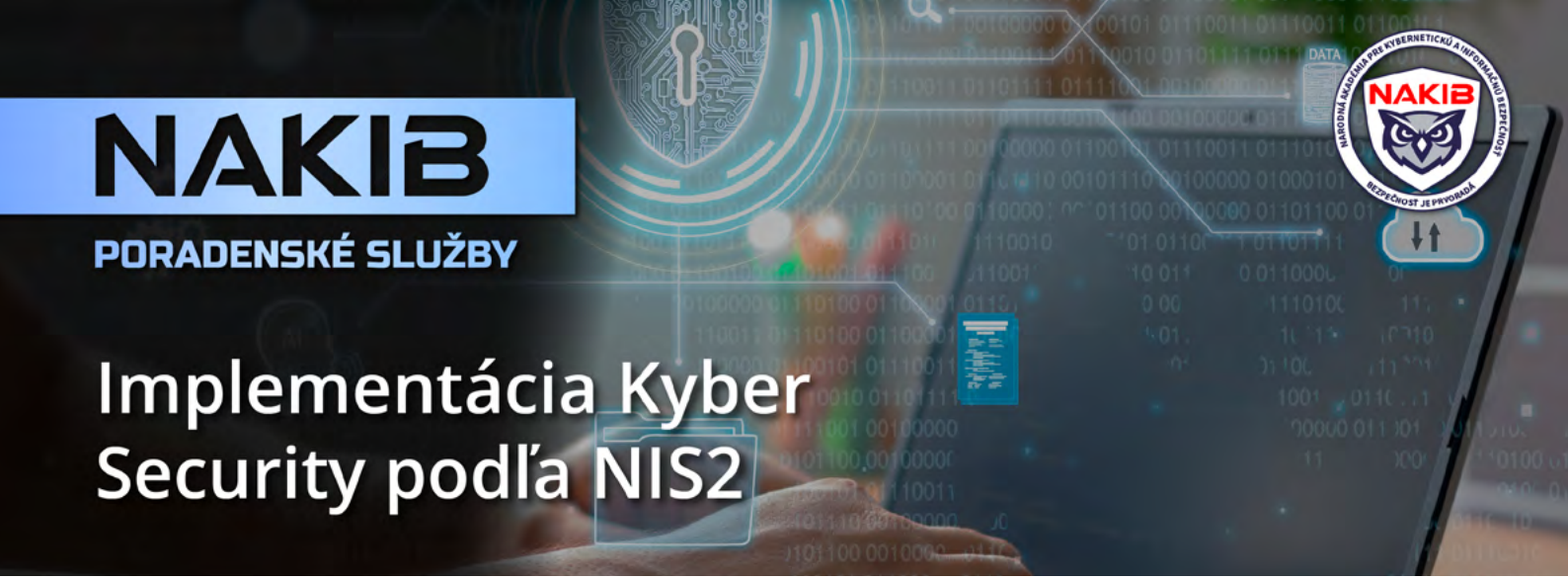
Implementácia kybernetickej bezpečnosti podľa ZoKB prináša viacero benefitov:
Zvýšenie ochrany informačných systémov a sietí: Znižuje sa riziko kybernetických útokov a narušení, čím sa chránia citlivé údaje a kritická infraštruktúra.
Posilnenie dôveryhodnosti a reputácie: Prevádzkovatelia demonštrujú zodpovedný prístup k ochrane informácií a budovaniu odolnosti voči kybernetickým hrozbám.
Zníženie rizika finančných a reputačných strát: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky a chráni reputáciu organizácie.
Spolnenie zákonných požiadaviek: Implementácia ZoKB je povinná pre prevádzkovateľov základných služieb a orgány verejnej moci.

Pre koho?

Zákon sa týka nasledovných subjektov:
Prevádzkovatelia základných služieb: Poskytovatelia kritických služieb v oblastiach ako energetika, doprava, financie, zdravotníctvo a digitálne služby.
Orgány verejnej moci: Štátne orgány, samosprávy a verejnoprávne inštitúcie.

Prínosy?

Implementácia kybernetickej bezpečnosti podľa ZoKB prináša nasledovné prínosy:
Zvýšená ochrana: Znižuje sa riziko krádeže dát, výpadkov služieb a narušenia prevádzky.
Posilnená odolnosť: Organizácia je lepšie pripravená na odrazenie a reakciu na kybernetické incidenty.
Zvýšená dôvera: Zákazníci a partneri vnímajú organizáciu ako zodpovednú a dôveryhodnú.
Zníženie nákladov: Predchádzanie incidentom a minimalizácia ich dopadov šetrí finančné prostriedky.



PORADENSTVO A POSKYTOVANIE SLUŽIEB V OBLASTI KYBER SECURITY NIS

Čo je?

Smernica o opatreniach na vysokú úroveň kybernetickej bezpečnosti v Únii (NIS2) je aktualizovaná legislatíva EÚ, ktorá nahradila pôvodnú smernicu NIS z roku 2016.

Prečo?

Implementácia kybernetickej bezpečnosti podľa NIS2 prináša viacero benefitov:
Zvýšená ochrana kľúčových sektorov: Posilňuje sa ochrana kritickej infraštruktúry a služieb v oblastiach ako energetika, doprava, financie, zdravotníctvo a digitálne služby.
Zvýšená odolnosť: Organizácie sú lepšie pripravené na odrazenie a reakciu na kybernetické incidenty.
Posilnená dôvera: Zákazníci a partneri vnímajú organizáciu ako zodpovednú a dôveryhodnú.
Zníženie rizika sankcií: Nesplnenie požiadaviek NIS2 môže viesť k sankciám zo strany regulačných orgánov.

Pre koho?

NIS2 sa týka nasledovných subjektov:
Prevádzkovatelia tzv. “**esenciálnych služieb**”: Poskytovatelia kritických služieb v oblastiach ako energetika, doprava, financie, zdravotníctvo a digitálne služby.
“**Dôležití poskytovatelia služieb**”: Poskytovatelia digitálnych služieb, ako sú online obchody, vyhľadávače a cloudové služby.

Prínosy?

Implementácia kybernetickej bezpečnosti podľa NIS2 prináša nasledovné prínosy:
Zvýšená ochrana: Znižuje sa riziko krádeže dát, výpadkov služieb a narušenia prevádzky.
Posilnená odolnosť: Organizácia je lepšie pripravená na odrazenie a reakciu na kybernetické incidenty.
Zvýšená dôvera: Zákazníci a partneri vnímajú organizáciu ako zodpovednú a dôveryhodnú.
Zníženie rizika sankcií: Splnenie požiadaviek NIS2 chráni pred sankciami zo strany regulačných orgánov.

PORADENSTVO ISMS (SYSTÉM RIADENIA KVALITY), PLATNOSŤ CERTIFIKÁCIE 3 ROKY, DOZORNÝ AUDIT ROČNE

Čo je?

ISO 9001 je medzinárodná norma pre systémy manažérstva kvality. Poskytuje súbor požiadaviek a osvedčených postupov, ktoré pomáhajú organizáciám efektívne riadiť a zlepšovať svoje procesy s cieľom dosiahnuť **trvalé uspokojenie zákazníkov**.

Prečo?

Implementácia ISO 9001 prináša viacero benefitov:
Zlepšenie kvality produktov a služieb: Systém manažérstva kvality pomáha organizácii identifikovať a eliminovať chyby v procesoch, čím sa zvyšuje kvalita produktov a služieb.
Zvýšenie spokojnosti zákazníkov: Zameranie na požiadavky a očakávania zákazníkov vedie k ich vyššej spokojnosti a lojalite. **Zvýšenie efektivity procesov:** Optimalizácia procesov a eliminácia plytvania vedie k zníženiu nákladov a zlepšeniu produktivity. **Posilnenie konkurencieschopnosti:** Implementácia ISO 9001 demonštruje záväzok organizácie k trvalému zlepšovaniu a posilňuje jej reputáciu na trhu. Zjednodušenie prístupu k tendrom: Mnoho verejných obstarávaní vyžaduje od uchádzačov certifikáciu ISO 9001.

Pre koho?

Norma ISO 9001 je univerzálna a môže sa **implementovať v akomkoľvek type organizácie**, bez ohľadu na jej veľkosť, oblasť pôsobnosti alebo stupeň zrelosti. Je vhodná pre:
Výrobné firmy: Zlepšuje riadenie výrobných procesov a kvalitu produktov.
Poskytovateľov služieb: Zlepšuje kvalitu služieb a zákaznícky servis.
Neziskovky: Zvyšuje efektivitu a transparentnosť fungovania organizácie.
Verejný sektor: Zlepšuje kvalitu verejných služieb a zodpovednosť voči občanom.

Prínosy?

Implementácia ISO 9001 prináša nasledovné prínosy:

Zvýšená dôvera: Zákazníci a partneri vnímajú organizáciu ako zodpovednú a spoľahlivú.
Lepšie riadenie rizík: Systém manažérstva kvality pomáha predchádzať chybám a eliminovať riziká.
Motivácia zamestnancov: Zapojenie zamestnancov do procesu zlepšovania posilňuje ich motiváciu a lojalitu.
Zlepšenie firemnej kultúry: Zameranie na kvalitu a neustále zlepšovanie vytvára pozitívnu firemnú kultúru.

PORADENSTVO V OBLASTI PRÍPRAVY NA CERTIFIKÁCIU ISMS (SYSTÉM RIADENIA INFORMAČNEJ BEZPEČNOSTI)

Čo je?

ISO/IEC 27001 je medzinárodná norma pre systémy manažérstva informačnej bezpečnosti. Poskytuje súbor požiadaviek a osvedčených postupov, ktoré pomáhajú organizáciám chrániť svoje informačné aktíva pred rôznymi hrozbami a incidentmi.

Prečo?

Implementácia ISO/IEC 27001 prináša viacero benefitov:
Zvýšenie informačnej bezpečnosti: Systém manažérstva informačnej bezpečnosti pomáha organizácii identifikovať a riadiť riziká týkajúce sa dôvernosti, integrity a dostupnosti informácií. Zníženie rizika kybernetických útokov: Implementácia kontrolných mechanizmov a osvedčených postupov znižuje riziko úspešných kybernetických útokov a narušenia informačných systémov. Posilnenie dôvery zákazníkov a partnerov: Certifikácia ISO/IEC 27001 demonštruje záväzok organizácie k ochrane informácií a posilňuje jej reputáciu na trhu. Zlepšenie súladu s regulačnými požiadavkami: Norma ISO/IEC 27001 integruje požiadavky rôznych regulačných predpisov na ochranu osobných údajov a informačnej bezpečnosti.
Zvýšenie efektivity riadenia informácií: Implementácia systému manažérstva informačnej bezpečnosti vedie k efektívnejšiemu riadeniu a ochrane informačných aktív.

Pre koho?

Norma ISO/IEC 27001 je univerzálna a môže sa implementovať v akomkoľvek type organizácie, bez ohľadu na jej veľkosť, oblasť pôsobnosti alebo stupeň zrelosti. Je vhodná pre:
Súkromné firmy: Zlepšuje ochranu citlivých informácií a obchodných tajomstiev.
Verejné inštitúcie: Zvyšuje bezpečnosť a dôveryhodnosť pri práci s citlivými údajmi občanov.
Neziskovky: Chráni informácie o darcoch, klientoch a interných procesoch.
Organizácie v regulovaných odvetviach: Uľahčuje splnenie požiadaviek na ochranu osobných údajov a informačnej bezpečnosti.

Prínosy?

Implementácia ISO/IEC 27001 prináša nasledovné prínosy:
Zníženie nákladov: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Zvýšenie produktivity: Zníženie výpadkov a narušení prevádzky súvisiacich s informačnou bezpečnosťou. Posilnenie konkurencieschopnosti: Demonštrovanie záväzku k ochrane informácií a budovanie odolnosti voči kybernetickým hrozbám. Zlepšenie firemnej kultúry: Zvýšenie povedomia o informačnej bezpečnosti a zodpovednosti zamestnancov.

NAKIB

PORADENSKÉ SLUŽBY

Implementácia ISO 27005

PORADENSTVO V OBLASTI RIADENIA RIZÍK AKO MANDATORNEJ POVINNOSTI PRE ISO 9K1, ISO 27K1, GDPR

Čo je?

ISO/IEC 27005 je medzinárodná norma, ktorá poskytuje usmernenia pre riadenie rizík informačnej bezpečnosti v súlade s normou ISO/IEC 27001. Norma definuje procesy a postupy na identifikáciu, hodnotenie a riadenie rizík súvisiacich s informačnými aktívami organizácie.

Prečo?

Implementácia ISO/IEC 27005 prináša viacero benefitov:
Zlepšenie riadenia rizík: Norma poskytuje systematický prístup k identifikácii, analýze a riadeniu rizík informačnej bezpečnosti. Zvýšenie efektívnosti: Optimalizácia procesov riadenia rizík znižuje čas a náklady na riešenie bezpečnostných incidentov. Posilnenie súladu s normami: Implementácia ISO/IEC 27005 podporuje súlad s požiadavkami ISO/IEC 27001 a ostatných regulačných predpisov. Zvýšenie informovanosti manažmentu: Poskytuje manažmentu jasný prehľad o rizikách informačnej bezpečnosti a ich dopadoch na organizáciu. Zlepšenie firemnej kultúry: Podporuje zodpovedné správanie zamestnancov pri práci s informáciami.

Pre koho?

Norma ISO/IEC 27005 je určená pre organizácie, ktoré už implementovali systém manažérstva informačnej bezpečnosti podľa ISO/IEC 27001 a chcú posilniť riadenie rizík v tejto oblasti. Je vhodná pre:
Súkromné firmy: Zlepšuje riadenie rizík súvisiacich s ochranou citlivých informácií a obchodných tajomstiev.
Verejné inštitúcie: Zvyšuje efektivitu riadenia rizík pri práci s citlivými údajmi občanov.
Neziskovky: Posilňuje ochranu informácií o darcoch, klientoch a interných procesoch.
Organizácie v regulovaných odvetviach: Uľahčuje splnenie požiadaviek na ochranu osobných údajov a informačnej bezpečnosti.

Prínosy?

Implementácia ISO/IEC 27005 prináša nasledovné prínosy:
Zníženie rizika kybernetických útokov: Lepšie pochopenie a riadenie rizík znižuje pravdepodobnosť úspešných kybernetických útokov. Zníženie finančných strát: Predchádzanie incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Posilnenie reputácie: Demonštrovanie záväzku k proaktívnemu riadeniu rizík posilňuje dôveru zákazníkov a partnerov.Zvýšenie konkurencieschopnosti: Zlepšenie odolnosti voči kybernetickým hrozbám a ochrana kľúčových informácií.

NAKIB

PORADENSKÉ SLUŽBY

Implementácia ISO 20000

PORADENSTVO V OBLASTI PRÍPRAVY NA CERTIFIKÁCIU (SYSTÉM RIADENIA ICT SLUŽIEB)

Čo je?

ISO 20000-1 je medzinárodná norma, ktorá definuje požiadavky na systém manažérstva služieb IT (SMS). Norma stanovuje súbor osvedčených postupov pre efektívne riadenie a dodávanie IT služieb v súlade s požiadavkami zákazníkov a s ohľadom na neustále zlepšovanie.

Prečo?

Implementácia ISO 20000-1 prináša viacero benefitov:
Zvýšenie kvality IT služieb: Norma podporuje systematický prístup k riadeniu IT služieb, čím sa zvyšuje ich kvalita a spoľahlivosť. Zlepšenie spokojnosti zákazníkov: Zameranie na požiadavky a očakávania zákazníkov vedie k ich vyššej spokojnosti a lojalite. Zvýšenie efektivity procesov: Optimalizácia procesov a eliminácia plytvania vedie k zníženiu nákladov a zlepšeniu produktivity. Posilnenie konkurencieschopnosti: Implementácia ISO 20000-1 demonštruje záväzok organizácie k trvalému zlepšovaniu a posilňuje jej reputáciu na trhu. Zjednodušenie prístupu k tendrom: Mnoho verejných obstarávaní v oblasti IT vyžaduje od uchádzačov certifikáciu ISO 20000-1.

Pre koho?

Norma ISO 20000-1 je univerzálna a môže sa implementovať v akomkoľvek type organizácie, ktorá poskytuje IT služby, bez ohľadu na jej veľkosť, oblasť pôsobnosti alebo stupeň zrelosti.
Je vhodná pre:
Poskytovateľov IT služieb: Zlepšuje riadenie a dodávanie IT služieb rôznym typom klientov.
Interné IT oddelenia: Zvyšuje efektivitu a kvalitu interných IT služieb v rámci organizácie.
Vývojárske firmy: Zlepšuje procesy vývoja a dodávania softvéru.
Organizácie s rozsiahlymi IT systémami: Posilňuje riadenie a kontrolu nad komplexnou IT infraštruktúrou.

Prínosy?

Implementácia ISO 20000-1 prináša nasledovné prínosy:
Zvýšenie dôvery: Zákazníci a partneri vnímajú organizáciu ako zodpovednú a spoľahlivú.
Lepšie riadenie rizík: Systém manažérstva služieb IT pomáha predchádzať incidentom a eliminovať riziká súvisiace s IT službami. Motivácia zamestnancov: Zapojenie zamestnancov do procesu zlepšovania posilňuje ich motiváciu a lojalitu. Zlepšenie firemnej kultúry: Zameranie na kvalitu a neustále zlepšovanie vytvára pozitívnu firemnú kultúru v oblasti IT.

PORADENSTVO V OBLASTI PRÍPRAVY NA CERTIFIKÁCIU (PRIEMYSELNA BEZPEČNOSŤ)

Čo je?

IEC 62443 je séria medzinárodných noriem, ktorá definuje požiadavky na kybernetickú a informačnú bezpečnosť priemyselných automatizačných a riadiacich systémov (IACS). Tieto normy stanovujú súbor osvedčených postupov pre ochranu IACS pred rôznymi hrozbami a incidentmi.

Prečo?

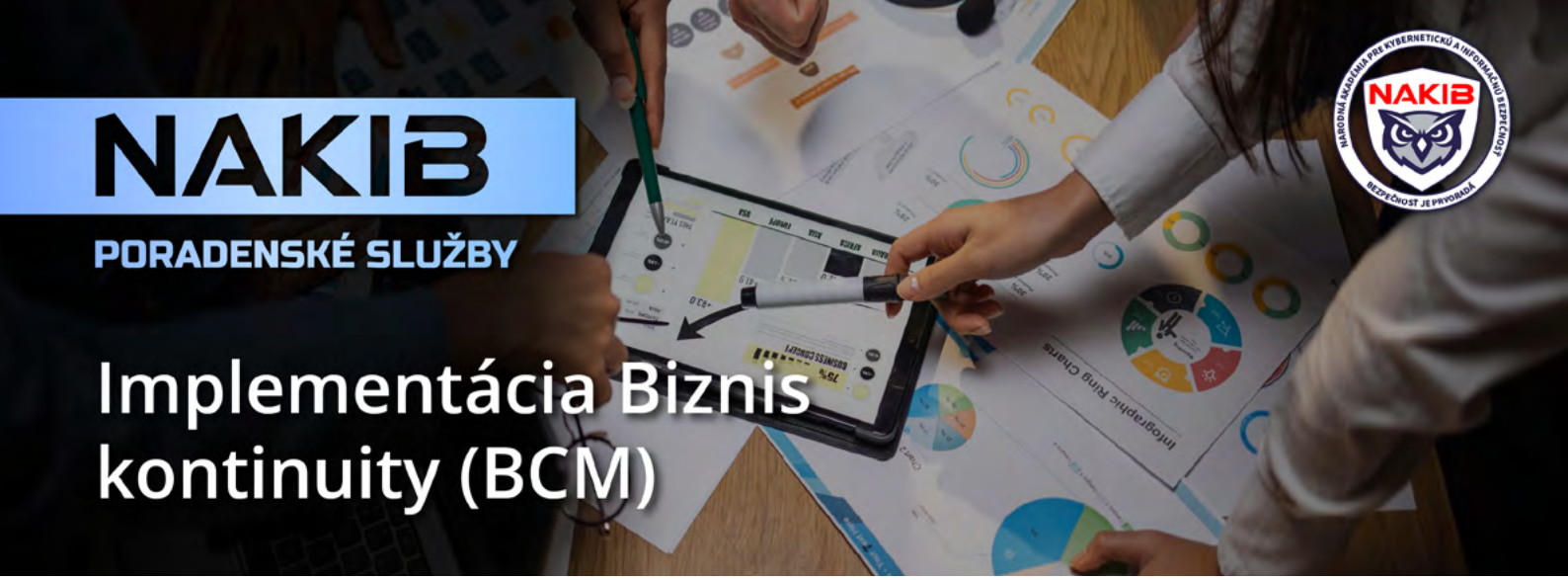
Implementácia IEC 62443 prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti IACS: Normy definujú komplexné bezpečnostné opatrenia na ochranu IACS pred kybernetickými útokmi a narušeniami.
Zníženie rizika výpadkov a porúch: Zvýšená odolnosť IACS znižuje riziko výpadkov prevádzky a porúch, ktoré by mohli viesť k značným finančným stratám.
Posilnenie súladu s regulačnými požiadavkami: IEC 62443 integruje požiadavky rôznych regulačných predpisov na kybernetickú bezpečnosť v priemyselnom sektore.
Zlepšenie ochrany kritickej infraštruktúry: Implementácia noriem posilňuje ochranu kritickej infraštruktúry, ako sú elektrárne, vodárenské systémy a dopravné systémy.
Zvýšenie dôvery a reputácie: Demonštrovanie záväzku k kybernetickej bezpečnosti posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu.

Pre koho?

Norma IEC 62443 je určená pre prevádzkovateľov a vlastníkov IACS v rôznych priemyselných odvetviach, ako sú: Energetika: Elektrárne, distribučné siete, prenosové sústavy.
Doprava: Letecká doprava, železničná doprava, cestná doprava, vodná doprava.
Vodárenstvo: Vodárenské systémy, čističky odpadových vôd.
Výroba: Automobilový priemysel, chemický priemysel, farmaceutický priemysel.
Kritická infraštruktúra: Ropovodné a plynové systémy, telekomunikácie, systémy riadenia budov.

Prínosy?

Implementácia IEC 62443 prináša nasledovné prínosy:
Zníženie nákladov: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky.
Zvýšenie produktivity: Zníženie výpadkov a narušení prevádzky súvisiacich s kybernetickou bezpečnosťou.
Posilnenie konkurencieschopnosti: Demonštrovanie záväzku k ochrane IACS a budovanie odolnosti voči kybernetickým hrozbám.
Zlepšenie firemnej kultúry: Zvýšenie povedomia o kybernetickej bezpečnosti a zodpovednosti zamestnancov.



NAKIB

PORADENSKÉ SLUŽBY

Implementácia Biznis kontinuity (BCM)

PORADENSTVO V OBLASTI PRÍPRAVY NA CERTIFIKÁCIU BIZNIS KONTINUITA PODĽA ISO 22301

Čo je?

BCM, skrátene pre Business Continuity Management, je strategický rámec pre riadenie kontinuity podnikania. Zahŕňa súbor procesov a aktivít, ktoré zaisťujú schopnosť poskytovania služieb aj počas krízy.

Prečo?

Implementácia BCM prináša viacero benefitov:
Zvýšenie odolnosti voči krízovým situáciám: BCM umožňuje organizácii rýchlo a efektívne reagovať na neočakávané udalosti a minimalizovať ich dopad na prevádzku. Zníženie rizika strát: Rýchle obnovenie kritických funkcií znižuje finančné straty a reputáciu, ktoré by mohli vzniknúť v dôsledku výpadku. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k kontinuite podnikania posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie firemnej kultúry: Zvýšenie povedomia o dôležitosti kontinuity podnikania a zodpovednosti zamestnancov. Spĺňanie regulačných požiadaviek: V niektorých odvetviach je implementácia BCM legislatívne podmienená.

Pre koho?

BCM je relevantný pre všetky typy organizácií, bez ohľadu na ich veľkosť, oblasť pôsobnosti alebo stupeň zrelosti. Je obzvlášť dôležitý pre:
Organizácie s kritickou infraštruktúrou: Poskytovatelia energií, telekomunikácií, dopravy a ďalších kritických služieb musia mať zaistenú kontinuitu prevádzky aj v krízových situáciách. Finančné inštitúcie: Banky, poisťovne a iné finančné inštitúcie musia chrániť svoje dáta a systémy pred narušením a výpadkami.
Veľké a komplexné organizácie: Rozsiahle firmy s rozsiahlymi sieťami a systémami potrebujú robustný systém riadenia kontinuity podnikania. Organizácie v regulovaných odvetviach: V niektorých odvetviach je implementácia BCM legislatívne podmienená.

Prínosy?

Implementácia BCM prináša nasledovné prínosy:
Zníženie nákladov: Predchádzanie stratám a minimalizácia dopadov krízových udalostí šetrí finančné prostriedky. Zvýšenie produktivity: Rýchle obnovenie prevádzky po krízových udalostiach minimalizuje straty produktivity. Posilnenie konkurencieschopnosti: Demonštrovanie odolnosti voči krízovým situáciám posilňuje konkurenčnú pozíciu organizácie. Zlepšenie morálky zamestnancov: Vedomie, že organizácia je pripravená na krízové situácie, zvyšuje morálku a motiváciu zamestnancov.

NAKIB

PORADENSKÉ SLUŽBY

Implementácia požiadaviek GDPR

PORADENSTVO V OBLASTI PRÍPRAVY NA ZABEZPEČENIE SÚLADU S NARIADENÍM GDPR

Čo je?

GDPR je skratka pre General Data Protection Regulation, v slovenčine nazývané aj Všeobecné nariadenie o ochrane údajov. Jedná sa o nariadenie Európskej únie, ktoré stanovuje pravidlá pre spracovanie osobných údajov fyzických osôb na území EÚ. Cieľom GDPR je chrániť súkromie a základné práva a slobody fyzických osôb a zároveň uľahčiť voľný pohyb osobných údajov v rámci EÚ.

Prečo?

Implementácia GDPR prináša viacero benefitov:
Zvýšenie ochrany osobných údajov: GDPR stanovuje prísne požiadavky na spracovanie osobných údajov, čím sa zvyšuje ich ochrana pred zneužitím. Zníženie rizika pokút: Porušenie GDPR môže viesť k vysokým pokutám, preto je dôležité mať implementované adekvátne bezpečnostné opatrenia. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k ochrane osobných údajov posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie firemnej kultúry: Zvýšenie povedomia o dôležitosti ochrany osobných údajov a zodpovednosti zamestnancov. Spĺňanie regulačných požiadaviek: GDPR je záväzné pre všetky organizácie, ktoré spracúvajú osobné údaje fyzických osôb v EÚ.

Pre koho?

GDPR sa vzťahuje na všetky organizácie, ktoré spracúvajú osobné údaje fyzických osôb v EÚ, bez ohľadu na ich veľkosť, oblasť pôsobnosti alebo sídlo. To zahŕňa:
Súkromné firmy: Všetky firmy, ktoré spracúvajú osobné údaje svojich zákazníkov, zamestnancov, dodávateľov a ďalších osôb. Verejné inštitúcie: Štátne orgány, úrady a verejné inštitúcie, ktoré spracúvajú osobné údaje v rámci svojej činnosti. Neziskovky: Neziskové organizácie a združenia, ktoré spracúvajú osobné údaje svojich členov, darcov a dobrovoľníkov. Fyzické osoby: Aj fyzické osoby, ktoré spracúvajú osobné údaje v rámci svojej profesie alebo inej činnosti.

Prínosy?

Implementácia GDPR prináša nasledovné prínosy:
Zníženie nákladov: Predchádzanie sankciám za porušenie GDPR a minimalizácia dopadov incidentov súvisiacich s ochranou osobných údajov šetrí finančné prostriedky. Zvýšenie produktivity: Zvýšenie efektivity spracovania osobných údajov a zníženie administratívnej záťaže. Posilnenie konkurencieschopnosti: Demonštrovanie zodpovedného prístupu k ochrane osobných údajov posilňuje konkurenčnú pozíciu organizácie na trhu. Zlepšenie imidžu a reputácie: Posilnenie dôvery verejnosti v organizáciu a jej záväzok k etickému spracovaniu osobných údajov.

PORADENSTVO V OBLASTI PRÍPRAVY NA AUDIT TISAX®

Čo je?

TISAX je skratka pre Trusted Information Security Assessment Exchange. Jedná sa o mechanizmus hodnotenia a výmeny informácií o informačnej bezpečnosti v automobilovom priemysle.

Prečo?

Implementácia TISAX prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti: TISAX stanovuje prísne požiadavky na riadenie informačnej bezpečnosti, čím sa znižuje riziko kybernetických útokov a narušení. Zlepšenie dodávateľského reťazca: TISAX umožňuje automobilovým výrobcom a dodávateľom zdieľať informácie o kybernetickej bezpečnosti a budovať dôveru v rámci dodávateľského reťazca. Zníženie nákladov: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Posilnenie konkurencieschopnosti: Demonštrovanie záväzku k informačnej bezpečnosti posilňuje konkurenčnú pozíciu na trhu automobilového priemyslu.
Spĺňanie požiadaviek odberateľov: Mnoho automobilových výrobcov a dodávateľov vyžaduje od svojich partnerov certifikáciu TISAX.

Pre koho?

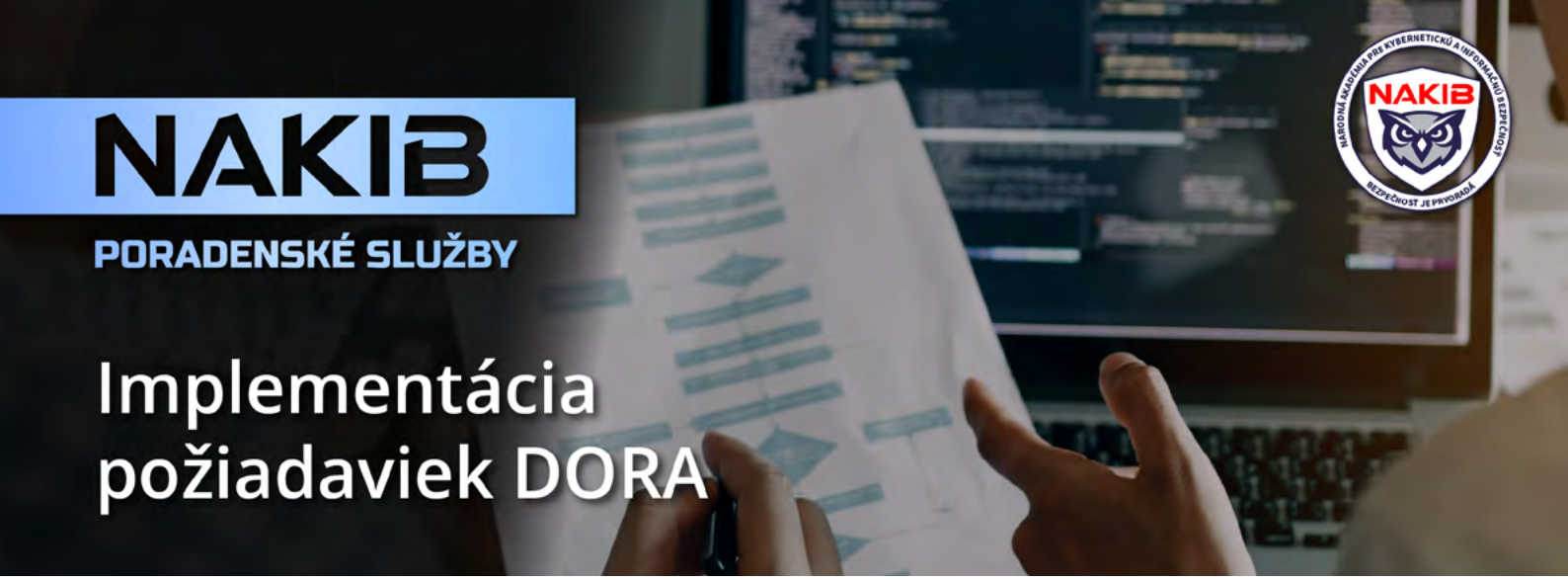
TISAX je určený pre všetky organizácie v automobilovom priemysle, ktoré spracúvajú citlivé informácie, ako napríklad:

Výrobcovia automobilov: OEM (Original Equipment Manufacturer) a Tier 1 dodávatelia.
Dodávatelia komponentov: Tier 2 a Tier 3 dodávatelia.
Poskytovatelia služieb: Poskytovatelia IT služieb, logistické firmy a iné subjekty v dodávateľskom reťazci.

Prínosy?

Implementácia TISAX prináša nasledovné prínosy:

Zvýšenie dôvery: Zákazníci a partneri vnímajú organizáciu ako zodpovednú a spoľahlivú v oblasti informačnej bezpečnosti.
Lepšie riadenie rizík: Systém manažérstva informačnej bezpečnosti TISAX pomáha predchádzať kybernetickým incidentom a eliminovať riziká súvisiace s informačnou bezpečnosťou.
Motivácia zamestnancov: Zapojenie zamestnancov do procesu zlepšovania informačnej bezpečnosti posilňuje ich motiváciu a lojalitu.
Zlepšenie firemnej kultúry: Zameranie na kybernetickú bezpečnosť a ochranu citlivých informácií vytvára pozitívnu firemnú kultúru.



PORADENSTVO V OBLASTI PRÍPRAVY NA MEDZINÁRODNÉHO ŠTANDARDU DORA PRE FINANČNÉ SLUŽBY

Čo je?

DORA je skratka pre Digital Operational Resilience Act, v slovenčine nazývané aj Akt o digitálnej prevádzkovej odolnosti. Jedná sa o nariadenie Európskej únie, ktoré stanovuje požiadavky na riadenie digitálnej prevádzkovej odolnosti (DORA) v sektore finančných služieb. Cieľom DORA je posilniť odolnosť finančného sektora voči digitálnym hrozbám a incidentom.

Prečo?

Implementácia DORA prináša viacero benefitov:
Zvýšenie odolnosti voči kybernetickým hrozbám: DORA stanovuje prísne požiadavky na riadenie digitálnych rizík, čím sa znižuje riziko kybernetických útokov a narušení prevádzky. Zníženie finančných strát: Predchádzanie incidentom a minimalizácia ich dopadov šetrí finančné prostriedky a chráni reputáciu finančných inštitúcií.Posilnenie dôvery a stability: Demonštrovanie záväzku k digitálnej odolnosti posilňuje dôveru zákazníkov a investorov v stabilitu finančného sektora.Zlepšenie súladu s regulačnými požiadavkami: DORA integruje požiadavky rôznych regulačných predpisov na kybernetickú a informačnú bezpečnosť v sektore finančných služieb.Zvýšenie konkurencieschopnosti: Implementácia DORA môže posilniť konkurenčnú pozíciu finančných inštitúcií, ktoré demonštrujú proaktívny prístup k riadeniu digitálnych rizík.

Pre koho?

DORA sa vzťahuje na všetky subjekty pôsobiace v sektore finančných služieb v EÚ, ako napríklad:
Banky: Všetky typy bánk, vrátane retailových bánk, investičných bánk a centrálnych bánk.
Poisťovne: Všetky typy poisťovní, vrátane životných poisťovní, neživotných poisťovní a zaisťovní.
Investičné firmy: Investičné fondy, správcovské spoločnosti, makléri a iné subjekty poskytujúce investičné služby. Platobné inštitúcie: Poskytovatelia platobných služieb, ako sú napríklad bankomaty, online platobné systémy a mobilné platby. Trhové infraštruktúry: Burzy cenných papierov, clearingové domy a depozitáre cenných papierov.

Prínosy?

Implementácia DORA prináša nasledovné prínosy:
Zníženie rizika výpadkov a porúch: Zvýšená odolnosť IT systémov a infraštruktúry znižuje riziko výpadkov prevádzky a porúch, ktoré by mohli viesť k značným finančným stratám. Lepšie riadenie incidentov: DORA definuje procesy a postupy pre efektívne riadenie kybernetických incidentov a minimalizáciu ich dopadov. Zvýšenie povedomia o kybernetickej bezpečnosti: Implementácia DORA zvyšuje povedomie o kybernetických hrozbách a dôležitosti ochrany citlivých informácií. Zlepšenie firemnej kultúry: Posilňuje zodpovednosť vedenia a zamestnancov za kybernetickú a informačnú bezpečnosť.

POSKYTOVANIE SLUŽIEB VULNERABILITY MANAGEMENTU ALEBO ZAVEDENIE PROCESU VULNERABILITY MANAŽMENT

Čo je?

Riadenie zraniteľností je systematický proces identifikácie, hodnotenia a riešenia zraniteľností v IT systémoch a softvéri. Cieľom riadenia zraniteľností je minimalizovať riziká kybernetických útokov a narušení prevádzky, ktoré by mohli viesť k finančným stratám, krádeži dát a strate reputácie.

Prečo?

Implementácia riadenia zraniteľností prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti: Riadenie zraniteľností znižuje riziko úspešných kybernetických útokov a narušení prevádzky. Zníženie finančných strát: Predchádzanie incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k kybernetickej bezpečnosti posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu.
Zlepšenie súladu s regulačnými požiadavkami: Mnoho regulačných predpisov vyžaduje od organizácií implementáciu riadenia zraniteľností. Zvýšenie produktivity: Zníženie výpadkov a porúch súvisiacich s kybernetickými útokmi.

Pre koho?

Riadenie zraniteľností je relevantné pre všetky typy organizácií, bez ohľadu na ich veľkosť, oblasť pôsobnosti alebo stupeň zrelosti. Je obzvlášť dôležité pre: Organizácie s kritickou infraštruktúrou: Poskytovatelia energií, telekomunikácií, dopravy a ďalších kritických služieb musia mať zaistenú ochranu svojich IT systémov pred zraniteľnosťami. Finančné inštitúcie: Banky, poisťovne a iné finančné inštitúcie musia chrániť svoje systémy a dáta pred kybernetickými útokmi. Veľké a komplexné organizácie: Rozsiahle firmy s rozsiahlymi sieťami a systémami potrebujú robustný systém riadenia zraniteľností. Organizácie v regulovaných odvetviach: V niektorých odvetviach je implementácia riadenia zraniteľností legislatívne podmienená.

Prínosy?

Implementácia riadenia zraniteľností prináša nasledovné prínosy:
Zníženie rizika kybernetických útokov: Včasná identifikácia a riešenie zraniteľností znižuje útočnú plochu pre hackerov. Rýchlejšia reakcia na incidenty: Schopnosť rýchlo identifikovať a reagovať na kybernetické incidenty minimalizuje ich dopady. Zlepšenie firemnej kultúry: Zvýšenie povedomia o kybernetických hrozbách a dôležitosti ochrany IT systémov. Lepšie riadenie IT rizík: Riadenie zraniteľností je dôležitou súčasťou celkového riadenia IT rizík v organizácii.

POSKYTOVANIE SLUŽIEB PENETRAČNÉHO TESTOVANIA

Čo je?

Penetráčné testy, skrátene PEN testy, sú simulované kybernetické útoky, ktoré sa vykonávajú s cieľom identifikovať a otestovať zraniteľnosti v IT systémoch a sieťach. Tieto testy sa realizujú z pohľadu útočníka.

Prečo?

Implementácia penetračných testov prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti: Penetráčné testy odhaľujú skryté zraniteľnosti v IT systémoch, ktoré by mohli byť zneužité hackermi. Zníženie rizika kybernetických útokov: Včasná identifikácia a riešenie zraniteľností znižuje útočnú plochu pre hackerov. Posilnenie dôvery a reputácie: Demonštrovanie záväzku k kybernetickej bezpečnosti posilňuje dôveru zákazníkov, partnerov a regulačných orgánov v organizáciu. Zlepšenie súladu s regulačnými požiadavkami: Mnoho regulačných predpisov vyžaduje od organizácií implementáciu penetračných testov. Zvýšenie efektivity IT infraštruktúry: Odhalenie a optimalizácia neefektívnych procesov v IT infraštruktúre.

Pre koho?

Penetráčné testy sú relevantné pre všetky typy organizácií, bez ohľadu na ich veľkosť, oblasť pôsobnosti alebo stupeň zrelosti. Je obzvlášť dôležité pre:
Organizácie s kritickou infraštruktúrou: Poskytovatelia energií, telekomunikácií, dopravy a ďalších kritických služieb musia mať zaistenú ochranu svojich IT systémov pred zraniteľnosťami.
Finančné inštitúcie: Banky, poisťovne a iné finančné inštitúcie musia chrániť svoje systémy a dáta pred kybernetickými útokmi. Veľké a komplexné organizácie: Rozsiahle firmy s rozsiahlymi sieťami a systémami potrebujú robustný systém riadenia kybernetickej bezpečnosti.
Organizácie v regulovaných odvetviach: V niektorých odvetviach je implementácia penetračných testov legislatívne podmienená.

Prínosy?

Implementácia penetračných testov prináša nasledovné prínosy:
Zníženie rizika finančných strát: Predchádzanie kybernetickým incidentom a minimalizácia ich dopadov šetrí finančné prostriedky. Zvýšenie produktivity: Zníženie výpadkov a porúch súvisiacich s kybernetickými útokmi. Posilnenie konkurencieschopnosti: Demonštrovanie proaktívneho prístupu k kybernetickej bezpečnosti posilňuje konkurenčnú pozíciu na trhu. Zlepšenie firemnej kultúry: Zvýšenie povedomia o kybernetických hrozbách a dôležitosti ochrany IT systémov.

PORADENSTVO A POSKYTOVANIE SLUŽIEB PRI VÝBERE A IMPLEMENTÁCII SIEM SYSTÉMOV

Čo je?

SIEM systém je softvérová platforma, ktorá integruje a analyzuje bezpečnostné informácie a udalosti z rôznych zdrojov v rámci IT infraštruktúry organizácie. SIEM systém umožňuje centralizované monitorovanie a riadenie bezpečnostných incidentov, čím zefektívňuje a urýchľuje reakciu na hrozby.

Prečo?

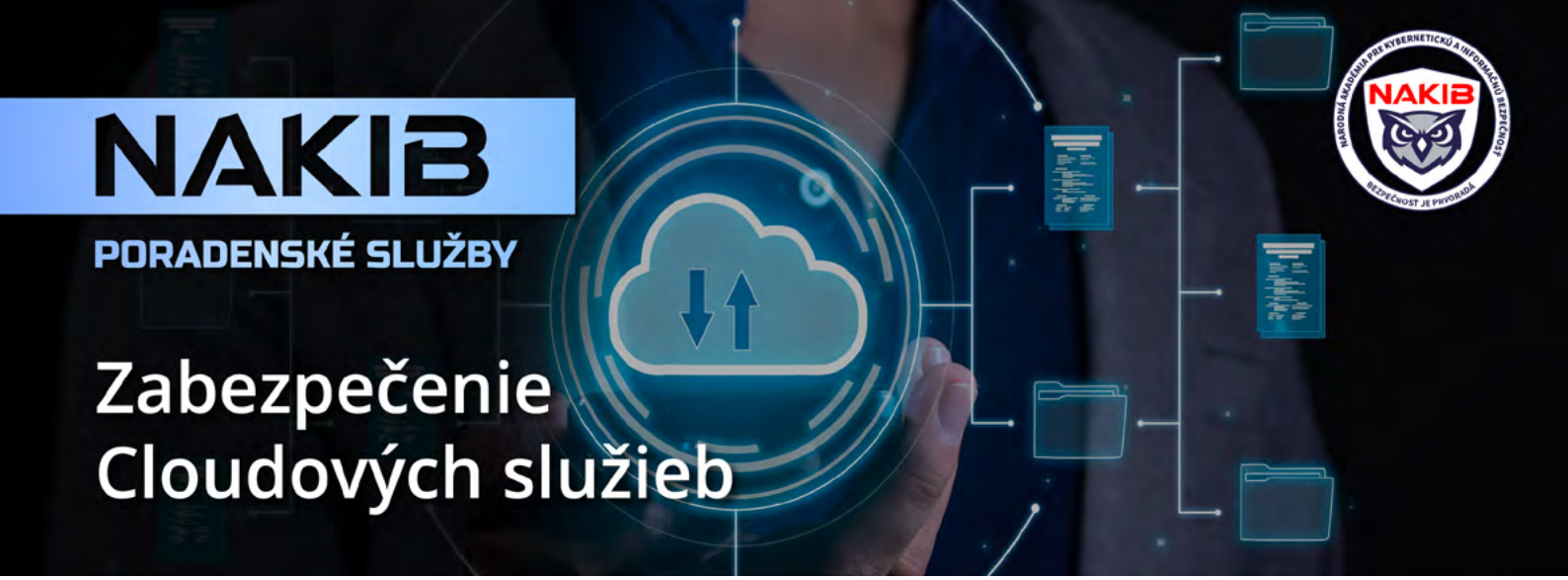
Implementácia SIEM systému prináša viacero benefitov:
Zvýšenie kybernetickej bezpečnosti: SIEM systém umožňuje včasnú detekciu a reakciu na kybernetické hrozby a incidenty. Zníženie rizika kybernetických útokov: Proaktívna identifikácia a analýza bezpečnostných udalostí znižuje útočnú plochu pre hackerov. Posilnenie súladu s regulačnými požiadavkami: Mnoho regulačných predpisov vyžaduje od organizácií implementáciu SIEM systému. Zníženie nákladov: Centralizovaná správa bezpečnostných informácií a udalostí znižuje náklady na riadenie kybernetickej bezpečnosti. Zlepšenie firemnej kultúry: Zvýšenie povedomia o kybernetických hrozbách a dôležitosti ochrany IT systémov.

Pre koho?

SIEM systém je relevantný pre všetky typy organizácií, bez ohľadu na ich veľkosť, oblasť pôsobnosti alebo stupeň zrelosti. Je obzvlášť dôležitý pre:
Organizácie s kritickou infraštruktúrou: Poskytovatelia energií, telekomunikácií, dopravy a ďalších kritických služieb musia mať zaistenú ochranu svojich IT systémov pred kybernetickými hrozbami.
Finančné inštitúcie: Banky, poisťovne a iné finančné inštitúcie musia chrániť svoje systémy a dáta pred kyberneticky mi útokmi.Veľké a komplexné organizácie: Rozsiahle firmy s rozsiahlymi sieťami a systémami potrebujú robustný systém riadenia kybernetickej bezpečnosti. Organizácie v regulovaných odvetviach: V niektorých odvetviach je implementácia SIEM systému legislatívne podmienená.

Prínosy?

Implementácia SIEM systému prináša nasledovné prínosy:
Zvýšenie rýchlosti a efektivity reakcie na incidenty: Centralizovaná analýza a korelácia udalostí umožňuje rýchlejšiu identifikáciu a reakciu na kybernetické incidenty. Zníženie objemu falošných poplachov: Inteligentná analýza udalostí znižuje počet falošných poplachov a umožňuje zamerať sa na relevantné hrozby. Zlepšenie forenznej analýzy: SIEM systém umožňuje zhromažďovať a analyzovať komplexné informácie o kybernetických incidentoch, čo uľahčuje forenznú analýzu a identifikáciu páchateľov.



NAKIB

PORADENSKÉ SLUŽBY

Zabezpečenie Cloudových služieb

PORADENSTVO V OBLASTI CLOUDOVÝCH SLUŽIEB A ICH ZABEZPEČENIA

Čo je?

Cloudové služby sú model dodávania IT služieb, ako napríklad úložisko dát, výpočtový výkon, softvér a databázy, cez internet. Tieto služby sú dostupné na požiadanie a škálovateľné podľa potreby, čím sa eliminuje potreba investovať do vlastnej IT infraštruktúry.

Prečo?

Zníženie nákladov: Cloudové služby eliminujú potrebu investovať do vlastného hardvéru a softvéru, znižujú náklady na údržbu a správu IT infraštruktúry. Zvýšenie flexibility a škálovatelnosti: Cloudové služby sa dajú rýchlo a jednoducho škálovať podľa aktuálnych potrieb, čím sa eliminuje potreba predimenzovávať vlastnú infraštruktúru. Zvýšená dostupnosť a spoľahlivosť: Cloudové služby sú dostupné 24/7 a poskytujú vysokú úroveň redundancie a ochrany dát. Zjednodušenie správy IT: Cloudové služby zjednodušujú správu IT infraštruktúry a umožňujú zamerať sa na strategické úlohy. Prístup k najnovším technológiám: Cloudové služby umožňujú prístup k najnovším IT technológiám bez potreby investovať do ich obstarania a údržby.

Pre koho?

Cloudové služby sú relevantné pre všetky typy organizácií, bez ohľadu na ich veľkosť, oblasť pôsobnosti alebo stupeň zrelosti. Sú vhodné pre:
Malé a stredné firmy: Cloudové služby umožňujú malým a stredným firmám prístup k moderným IT riešeniam bez potreby investovať do vlastnej infraštruktúry. Veľké firmy: Veľké firmy s rozsiahlymi IT požiadavkami dokážu využiť cloudové služby na zníženie nákladov a zjednodušenie správy IT.
Startupy a rýchlo rastúce firmy: Cloudové služby umožňujú startupom a rýchlo rastúcim firmám rýchlo a jednoducho škálovať svoju IT infraštruktúru podľa potreby.
Neziskovky a verejná správa: Cloudové služby sú vhodné pre Neziskovky a verejnú správu z dôvodu nízkych vstupných nákladov a vysokej škálovateľnosti.

Prínosy?

Implementácia cloudových služieb prináša nasledovné prínosy:
Zvýšenie produktivity: Zamestnanci sa možu sústrediť na svoje core úlohy a nemusia sa starať o správu IT infraštruktúry.
Zlepšenie spolupráce: Cloudové služby uľahčujú spoluprácu medzi zamestnancami a tímami, aj keď sa nachádzajú na rôznych miestach.
Zvýšená mobilita: Cloudové služby umožňujú prístup k firemným dátam a aplikáciám odkiaľkoľvek a z akéhokoľvek zariadenia.
Zvýšená bezpečnosť: Cloudové služby ponúkajú vysokú úroveň bezpečnosti a ochrany dát.