

System manažérstva bezpečnosti informácií (ISMS) v automobilovom priemysle

TÜV NORD CERT – Hodnotenie systému riadenia bezpečnosti informácií podľa TISAX



Moderné automobily obsahujú veľké množstvo sieťovo prepojených meracích a kontrolných zariadení. Bezpečnosť informácií tak nie je prioritou len u „mobilných počítačov“. Je takisto dôležitým faktorom vo vývoji, výrobných procesoch a pri výmene dát a informácií. Riadenie a znížovanie rizík pri ochrane dát a zaistenie ich integrity a dostupnosti je dosiahnuté prostredníctvom systému riadenia bezpečnosti informácií (ISMS).

V automobilovom priemysle môže byť účinnosť systému riadenia bezpečnosti informácií (ISMS) stanovená prostredníctvom hodnotenia podľa TISAX (Trusted Information Security Assessment Exchange), ktorú mnoho výrobcov automobilov vyžaduje ako záväznú podmienku. Hodnotenia sú založené na súbore požiadaviek podľa noriem VDA ISA, vyvinutých Nemeckým zväzom automobilového priemyslu (German Association of the Automotive Industry) VDA.

Prístup k zaisteniu bezpečnosti informácií vychádza z významných aspektov a kritérií medzinárodne uznávanej normy ISO 27001. Navyše boli zostavené zvláštne súbory požiadaviek, týkajúce sa zapojenia tretích strán a zaobchádzania s prototypmi. Zavedený proces výmeny informácií šitý na mieru poskytuje vysokú mieru porovnateľnosti a transparentnosti, a teda posilňuje dôveru zákazníkov, ktorí požadujú získať značku TISAX.

Existujú dve možné účastnícke role

Podľa potreby môžu zúčastnené strany v rámci výmeny dát zaujať dve role:

- Pasívny účastník (napr. OEM, výrobcovia automobilov): Pasívni účastníci vyžadujú, aby hodnotenie vykonala iná spoločnosť (napr. dodávateľ) a potom žiadajú o prístup k výsledkom hodnotenia.
- Aktívny účastník (napr. dodávateľ): Iná spoločnosť vyžaduje, aby aktívny účastník podstúpil hodnotenie podľa súboru požiadaviek, prípadne týmto hodnotením aktívny účastník prejde z vlastnej iniciatívy. Následne po hodnotení aktívny účastník umožní vybraným spoločnostiam (napr. OEM) prístup k výsledkom hodnotenia.

Prostredníctvom registrácie účastníka získajú spoločnosti prístup na portál TISAX. Registrácia je tiež nevyhnutným predpokladom, ak spoločnosť žiada, aby hodnotenie vykonala akreditovaná auditorská spoločnosť. Tieto organizácie sú známe pod označením XAP.

Rôzne úrovne zabezpečenia a hodnotenia a kroky skúšobného postupu

V závislosti na požadovanej miere zabezpečenia existujú rôzne úrovne hodnotenia ovplyvňujúce hodnotenie spoločnosti:

Úroveň hodnotenia 1 je dôležitá na interné účely v zmysle sebahodnotenia auditovaného subjektu.

V prípade vysokej miery zabezpečenia je vykonávané hodnotenie podľa úrovne 2, pričom účasť XAP je povinná. Predpokladom v tomto prípade je vykonané hodnotenie podľa úrovne 1, to znamená, že bolo vykonané sebahodnotenie v plnom rozsahu. Kroky hodnotenia úrovne 2 sú tieto:

- Úvodná schôdzka
- Kontrola úplnosti a hodnovernosti sebahodnotenia a vhodnosti dôkazov
- Telefonické dotazovanie osôb zodpovedných za systém riadenia bezpečnosti informácií (ISMS) na základe požadovaných dokumentov (kontrola na mieste, ak je to nutné - napr. pri zapojení tretích osôb a/alebo ochrany prototypu).

V prípade veľmi vysokej miery zabezpečenia je vykonávané hodnotenie podľa úrovne 3, ktoré musí zahŕňať účasť XAP. Kroky skúšobného postupu sú tu podobné ako pri úrovni hodnotenia 2 s tým, že sú počas kontroly na mieste posudzované významné aspekty. Samozrejmosťou je sebahodnotenie vykonané v plnom rozsahu:

- Úvodná schôdzka
- Kontrola úplnosti a hodnovernosti sebahodnotenia a vhodnosti dôkazov
- Hodnotenie efektívnosti a účelnosti ISMS prostredníctvom kontroly na mieste so zúčastnenými subjektmi (pohovory na mieste s odborníkmi, kontrola príslušných oblastí v organizácii).

Po vykonaní hodnotení na úrovniach 2 a 3 sú prebraté zistenia (napr. úroveň vyspelosti) a požiadavky na nápravné opatrenia a následne je ich zhrnutie uvedené v predbežnej správe.

Po úvodnom vyššie uvedenom posúdení musí byť za účelom získania značky TISAX vykonané hodnotenie v nasledujúcich dvoch krokoch:

- Auditovaný subjekt vypracuje plán nápravných opatrení, ktorý preskúma XAP. Formou aktualizácie predbežnej správy bude plán vysvetlený a zhrnutý v následnej správe.
- Zavedenie nápravných opatrení auditovaným subjektom a posúdenie opatrení zo strany XAP. Tu je taktiež zostavená správa (obvykle vo forme ďalšej aktualizácie), ktorá je následne nahraná na platformu ENX ako záverečná správa. Maximálna lehota od úvodného stretnutia po túto záverečnú fázu je deväť mesiacov. V prípade, že je táto lehota prekročená, celý proces musí byť zahájený znova od začiatku.

Každá spoločnosť sa môže sama rozhodnúť, komu budú výsledky sprístupnené. Kvalita hodnotiaceho procesu a zistenia je preskúmaná asociáciou ENX, ktorá následne udelí značku TISAX s platnosťou na tri roky. Po uplynutí tejto lehoty musí byť celý postup zopakovaný.

Cielové skupiny pre hodnotenie podľa TISAX

Hodnotenie podľa TISAX bolo vypracované pre dodávateľov a poskytovateľov služieb v automobilovom priemysle, ktorí pracujú s citlivými informáciami. Značku TISAX uznávajú všetci členovia Nemeckého zväzu automobilových výrobcov (VDA), vrátane spoločností ako Audi, Volkswagen, BMW a rad ďalších. V niektorých prípadoch je certifikácia TISAX považovaná za záväznú podmienku zmluvy s dodávateľmi.

Výhody programu TISAX

- Všetky hodnotiace kritériá sú relevantné pre automobilový priemysel
- Vysoká kvalita hodnotenia a konzistentné výsledky
- Štandardizované a prísne hodnotenie a postupy podávania správ
- Výsledky sú preto porovnateľné aj zmysluplné
- Možno vylúčiť duplicitné a opakované hodnotenie
- Zníženie rizík a zavedenie systému riadenia rizík
- Široké prijatie a väčšia dôvera v rámci automobilového sektora
- Vyššia miera lojality zákazníkov a podpora nového podnikania
- Silná orientácia na potreby zákazníkov

Naše know-how pre Váš úspech

Spoločnosť TÜV NORD CERT GmbH bola pred mnohými rokmi schválená nemeckým akreditačným orgánom DAkkS pre vykonávanie auditov a certifikácie systémov riadenia bezpečnosti informácií (ISMS) a na základe svojej odbornej spôsobilosti bola schválená spoločnosťou ENX akreditovaná auditorská spoločnosť TISAX (XAP) pre automobilový priemysel.

TÜV NORD Slovakia, s.r.o.

Dúbravská cesta 2

841 04 Bratislava

Tel.: +421 5341 6380

E-mail: info.sk@tuv-nord.com

www.tuvnord.sk