Systém managementu bezpečnosti informací (ISMS)
v automobilovém průmyslu

TÜV NORD CERT – Hodnocení systémů řízení bezpečnosti informací podle TISAX

Moderní vozidla obsahují velké množství síťově propojených měřících a kontrolních zařízení. Bezpečnost informací ovšem není prioritou pouze u „mobilních počítačů“. Je také důležitým faktorem ve vývoji, výrobních procesech a při výměně dat a informací. Řízení a snižování rizik při ochraně dat a zajištění jejich integrity a dostupnosti je dosaženo prostřednictvím systému řízení bezpečnosti informací (ISMS).

V automobilovém průmyslu může být účinnost systému řízení bezpečnosti informací (ISMS) stanovena prostřednictvím hodnocení podle TISAX (Trusted Information Security Assessment Exchange), které mnoho výrobců automobilů vyžaduje jako závaznou podmínku. Hodnocení jsou založena na souboru požadavků dle norem VDA ISA, vyvinutých Německým svazem automobilového průmyslu (German Association of the Automotive Industry) VDA.

Přístup k zajištění bezpečnosti informací vychází z významných aspektů a kritérií mezinárodně uznávané normy ISO 27001. Navíc byly sestaveny zvláštní soubory požadavků, týkající se zapojení třetích stran a zacházení s prototypy. Zavedený proces výměny informací šitý na míru poskytuje vysokou míru srovnatelnosti a transparentnosti, a tudíž posiluje důvěru zákazníků, kteří požadují získat značku TISAX.

Existují dvě možné účastnické role

Podle potřeby mohou zúčastněné strany v rámci výměny dat zaujmout dvě role:

- Pasivní účastník (např. OEM, výrobci automobilů): Pasivní účastníci vyžadují, aby hodnocení provedla jiná společnost (např. dodavatel) a poté žádají o přístup k výsledkům hodnocení.
- Aktivní účastník (např. dodavatel): Jiná společnost vyžaduje, aby aktivní účastník podstoupil hodnocení podle souboru požadavků, případně tímto hodnocením aktivní účastník projde z vlastní iniciativy. Následně po hodnocení aktivní účastník umožní vybraným společnostem (např. OEM) přístup k výsledkům hodnocení.

Prostřednictvím registrace účastníka získají společnosti přístup na portál TISAX. Registrace je také nezbytným předpokladem, pokud společnost žádá, aby hodnocení provedla akreditovaná auditorská společnost. Tyto organizace jsou známé pod označením XAP.

TÜV®

TÜV NORD
Czech

Různé úrovně zabezpečení a hodnocení a kroky zkušebního postupu

V závislosti na požadované míře zabezpečení existují různé úrovně hodnocení ovlivňující hodnocení společnosti:

Úroveň hodnocení 1 je důležitá pro interní účely ve smyslu sebehodnocení auditovaného subjektu.

V případě vysoké míry zabezpečení je prováděno hodnocení podle úrovně 2, přičemž účast XAP je povinná. Předpokladem v tomto případě je provedené hodnocení podle úrovně 1, to znamená, že bylo provedeno sebehodnocení v plném rozsahu. Kroky hodnocení úrovně 2 jsou tyto:

- Úvodní schůzka
- Kontrola úplnosti a hodnověrnosti sebehodnocení a vhodnosti důkazů
- Telefonické dotazování osob zodpovědných za systém řízení bezpečnosti informací (ISMS) na základě požadovaných dokumentů (kontrola na místě, je-li to nutné - např. při zapojení třetích osob a/ nebo ochrany prototypu).

V případě velmi vysoké míry zabezpečení je prováděno hodnocení podle úrovně 3, které musí zahrnovat účast XAP. Kroky zkušebního postupu jsou zde obdobné jako u úrovně hodnocení 2 s tím, že jsou během kontroly na místě posuzovány významné aspekty. Samozřejmostí je sebehodnocení provedené v plném rozsahu:

- Úvodní schůzka
- Kontrola úplnosti a hodnověrnosti sebehodnocení a vhodnosti důkazů
- Hodnocení efektivnosti a účelnosti ISMS prostřednictvím kontroly na místě se zúčastněnými subjekty (pohovory na místě s odborníky, kontrola příslušných oblastí v organizaci).

Po provedení hodnocení na úrovních 2 a 3 jsou probrána zjištění (např. úroveň vyspělosti) a požadavky na nápravná opatření a následně je jejich shrnutí uvedeno v předběžné zprávě.

Po úvodním výše uvedeném posouzení musí být za účelem získání značky TISAX provedeno hodnocení v následujících dvou krocích:

- Auditovaný subjekt vypracuje plán nápravných opatření, který přezkoumá XAP. Formou aktualizace předběžné zprávy bude plán vysvětlen a shrnut v následné zprávě.
- Zavedení nápravných opatření auditovaným subjektem a posouzení opatření ze strany XAP. Zde je taktéž sestavena zpráva (obvykle ve formě další aktualizace), která je následně nahrána na platformu ENX jako závěrečná zpráva. Maximální lhůta od úvodní schůzky po tuto závěrečnou fázi je devět měsíců. V případě, že je tato lhůta překročena, celý proces musí být zahájen znovu od začátku.

Každá společnost se může sama rozhodnout, komu budou výsledky zpřístupněny. Kvalita hodnotícího procesu a zjištění je přezkoumána asociací ENX, která následně udělí značku TISAX s platností na tři roky. Po uplynutí této lhůty musí být celý postup zopakován.

Cílové skupiny pro hodnocení podle TISAX

Hodnocení podle TISAX bylo vypracováno pro dodavatele a poskytovatele služeb v automobilovém průmyslu, kteří pracují s citlivými informacemi. Značku TISAX uznávají všichni členové Německého svazu automobilových výrobců (VDA), včetně společností jako Audi, Volkswagen, BMW a řada dalších. V některých případech je certifikace TISAX považována za závaznou podmínku smlouvy s dodavateli.

Výhody programu TISAX

- Všechna hodnotící kritéria jsou relevantní pro automobilový průmysl
- Vysoká kvalita hodnocení a konzistentní výsledky
- Standardizované a přísné hodnocení a postupy podávání zpráv
- Výsledky jsou proto srovnatelné i smysluplné
- Lze vyloučit duplicitní a opakované hodnocení
- Snížení rizik a zavedení systému řízení rizik
- Široké přijetí a větší důvěra v rámci automobilového sektoru
- Vyšší míra loajality zákazníků a podpora nového podnikání
- Silná orientace na potřeby zákazníků

Naše know-how pro Váš úspěch

Společnost TÜV NORD CERT GmbH byla před mnoha lety schválena německým akreditačním orgánem DAkkS pro provádění auditů a certifikace systémů řízení bezpečnosti informací (ISMS) a na základě své odborné způsobilosti byla schválena společností ENX akreditovaná auditorská společnost TISAX (XAP) pro automobilový průmysl.

Měli byste zájem o více informací?
Prosím, kontaktujte nás.
Pošlete nám prosím Vaši odpověď e-mailem.
Těšíme se na zprávu od Vás.

☐ **Ano, máme zájem o hodnocení systému řízení bezpečnosti informací podle TISAX.**

☐ **Chtěli bychom získávat pravidelné informace prostřednictvím newsletteru.**

Chci se rovnou přihlásit k bezplatnému odběru newsletteru

Odesílatel (Vyplňte, prosím, tiskacím písmem)

Společnost _____

Pán / Paní _____

Pozice _____

PSČ / Město _____

Ulice, číslo popisné _____

E-mail / Tel. _____

Odeslat formulář

Ing. Jiří Panáček
Ředitel divize certifikace systémů managementu

TÜV NORD Czech, s.r.o.
Českomoravská 2420/15
190 00 Praha 9
Tel.: +420 296 587 201-9
Mob.: +420 602 530 547
E-mail: panacek@tuev-nord.cz