Alverad Technology Focus Kft.
1138 Budapest,
Madarász Viktor u. 47–49., II./1.
www.alverad.hu
info@alverad.hu
+36 1 797 6689

ALVERAD
TECHNOLOGY FOCUS

IATF-16949 kiberbiztonság

QUALITY MANAGEMENT SYSTEM
IATF 16949

SECURITY TESTING LABORATORY
MAKING THE WORLD SAFER

Tartalom

Az IATF-16949 szabvány kiberbiztonsági aspektusai

Szabványváltozás

A 2016 októberében kiadott IATF-16949:2016 autóipari szabvány 2019. novemberi „Hivatalos értelmezése" (*Sanctioned Interpretations* – SI-16-18) 2020. januárjától érvényes, azaz a tanúsításkor már az új elvárásoknak is meg kell felelnie a szervezetnek.

Iparbiztonsági szempontból a legfontosabb változás, hogy a megfelelőséghez (ipari) kibervédelmi és kiberbiztonsági képességeket, funkciókat, eljárásokat is szükséges átláthatóan, auditálhatóan kiépíteni és működtetni.

Jelen összefoglaló a megjelent kiberbiztonsági elvárásokkal kapcsolatban nyújt segítséget azon szervezetek és vállalatok részére, akik a szabvány szerinti megfelelőségre törekednek.

A kiberbiztonsági funkciók megjelenése a szabványban

Gyártást támogató berendezések és rendszerek kiberbiztonsága kiegészítés

A szabvány 7.1.3.1 „*Telephely, létesítmény és berendezések tervezése*" (c) pontjában új elemként jelent meg, hogy a szervezetnek **„kibervédelmet kell bevezetnie a gyártást támogató berendezésekre és rendszerekre".**

A kiegészítés a klasszikus IT biztonság „*security-by-design*" elvének átültetéseként fogható fel. Az elv szerint egy új rendszer (telephely, berendezés) létesítésekor a szervezetnek már a tervezés szakaszában figyelemmel kell lennie a kiberbiztonság elveire, általános és specifikus elvárásaira.

A kiberbiztonság nem korlátozódik az irodai funkciókra és azok kontrolljaira. A gyártási területen alkalmazott eszközök, berendezések, számítógépek az irodai rendszerekhez hasonlóan ki vannak téve a kibertámadás veszélyének, amelyek a folyamatos működés és rendelkezésre állás mellett a vevői követelményeknek való megfelelést fenyegethetik.

Az értelmezés kiegészítése nem jelenti azt, hogy egy már meglévő gyártási rendszer vagy berendezés esetén nem szükséges a kibervédelmi és kiberbiztonsági funkciók megvalósítása. Más pontjaiban az értelmezés egyértelműsíti, hogy a kibervédelmi és kiberbiztonsági funkciók megvalósítását elvárja a megfelelőséghez.

Kiberbiztonsági tesztelés kiegészítés

A szabvány 6.1.2.3 „*Vészhelyzeti terv*" (e) pontjában új elemkén jelent meg **a kiberbiztonsági tesztelés fogalma és elvárása**. A kiberbiztonsági teszteléssel kapcsolatban több lehetőséget is felsorol a kiegészítés, magában foglalhatja a kibertámadás szimulációját, meghatározott fenyegetettségek rendszeres monitorozását, a függőségek azonosítását és a sérülékenységek priorizálását.

A kiegészítés rögzíti, hogy a kiberbiztonsági tesztelést végezheti maga a szervezet, de ki is szervezheti a tevékenységet, aszerint, hogy melyik a számára megfelelőbb és hatékonyabb opció.

Kibertámadások szimulációja

A kibertámadások valósághű szimulációja jellemzően a nagyobb szervezetek esetében kaphat szerepet. Például az ipari környezetekre és gyártási rendszerekre szabott, úgynevezett „*Red Teaming*" egy valós szimuláció, amely során a támadók a lehető legrealisztikusabb módszerekkel és eszközökkel igyekeznek megtámadni a védett hálózatot és eszközöket. A valósághű szimulációban a támadókat megszemélyesítő szakértők (Red team) gyakorlatilag bármilyen támadást alkalmazhatnak. Minél kevesebb az őket megkötő szabály, annál életszerűbb a szimuláció.

Ipari és gyártási környezetekben természetesen ilyen szimulációt megvalósítani nagyon sok előkészülettel, kockázattal és erőforrás felhasználással jár, ezért a kisebb szervezetek esetében inkább olyan tesztek lehetnek javasoltak, ahol a támadók és a védők egy úgynevezett „*tabletop*" szimulációban vesznek részt. Az ilyen „asztali" szimulációk során papíron, táblán vázolják fel a támadók a különféle támadási eljárásokat és taktikákat, amelyekre a védők is papíron vagy táblán reagálnak. A módszer bár nem teljesen valósághű, azonban a különféle védelmi és reagáló folyamatok tesztelésére tökéletesen alkalmas.

Meghatározott fenyegetések monitorozása

A fenyegetések felmérése a kockázatfeltáró és kockázatelemző tevékenység része. A feltárt fenyegetettségekre és kockázatokra a szervezetnek a kockázatkezelés során megfelelő csillapító intézkedéseket kell hoznia, amelyek arányosak a várható hatásokkal, valamint a vonatkozó vevői zavarok kockázatával.

Meghatározott fenyegetések lehetnek például (nem kizárólag):

- Eszköz, berendezés, rendszer ismert sérülékenységéből fakadó kockázatok
- Eszköz, berendezés, rendszer nem ismert sérülékenységéből fakadó kockázatok
- Elavult, nem frissíthető rendszerekből adódó kockázatok
- Malware- és vírus-fenyegetettség (például ransomware, infostealer, stb)
- Távelérésből fakadó kockázatok
- Ismeretlen eszközök csatlakoztatásából fakadó kockázatok
- Jogosulatlan hozzáférések kockázatai
- Szabotázs lehetőségének kockázata
- Jogosulatlan programletöltés kockázata
- Rosszindulatú programmódosítás kockázata,
- Stb.

Függőségek azonosítása

A függőségek azonosítása az egymással kapcsolódó rendszerek, illetve folyamatok függőségeinek azonosítását jelenti.

A szolgáltatási lánc védelme ebből a szempontból egyrészt azt jelenti, hogy a szervezetnek azonosítania kell azon rendszereit, eszközeit és folyamatait, amelyek a vevő(k) kiszolgálásához technológiailag, üzletileg, illetve természetesen a minőségirányítási kontroll szempontjából kritikus fontosságúak, másrészt a feltárt függőségeket és egymásra gyakorolt hatásukat a bizalmasság, sértetlenség és rendelkezésre állás szempontjából is meg kell vizsgálni.

Sérülékenységek priorizációja

A kiegészítés egyik legfontosabb pontja a sérülékenységek beemelése és megjelenítése. A kiegészítés hivatkozik arra, hogy a kiberbiztonság a gyártás fenntartásának szempontjából egyre fokozódó kockázatot jelent, ennek fényében pedig a sérülékenységek priorizációjának elvárása - véleményünk szerint - különösen nagy hangsúlyt kap.

A sérülékenységek priorizálásához ugyanis először fel kell mérni a gyártási rendszer, eszközök és berendezések sérülékenységeit, és a sérülékenységvizsgálat eredményterméke fogja tartalmazni:

- a feltárt sérülékenységeket,
- a sérülékenységek üzemi folyamatokra és az üzleti célokra gyakorolt kockázatait és hatásait,
- a sérülékenységek súlyosság vagy hatás alapú priorizálását,
- valamint a sérülékenységek javítását célzó javaslatokat és intézkedéseket.

A korábban ismertetett függőségekkel kapcsolatos pontra visszautalva látható, hogy már a függőségek egymásra gyakorolt hatásainak értékeléséhez is szükség lehet a sérülékenységek azonosítására, hiszen egy-egy rendszerelem kiesése bekövetkezhet a rendszerelem vagy más rendszerelemek valamely sérülékenységét kihasználó kibertámadás miatt.

A sérülékenységvizsgálat tehát kiemelt fontosságú az ipari és gyártási rendszerek kiberbiztonságát tekintve. A sérülékenységek és a kibervédelem egyéb hiányosságainak kihasználásával nem csak egy adott rendszer kerülhet veszélybe, de a függőségeken keresztül a szolgáltatási lánc is megszakadhat.

Esemény- és incidenskezelés kiegészítés

A szabvány 6.1.2.3 „*Vészhelyzeti terv*" (c) pontjában új elemként jelent meg, hogy a Vészhelyzeti tervnek intézkedéseket kell tartalmaznia a kibertámadás-típusú eseményekre

vonatkozóan. A változás indoklásában a kiegészítés kifejti, hogy a szervezetnek foglalkoznia kell a kibertámadás lehetőségével és a szervezetnek biztosítania kell, hogy felkészült legyen egy bekövetkező kibertámadással szemben.

Ez olyan eljárások kialakítását, dokumentálását és begyakorlását jelenti, amelyekkel a szervezet képes:

- reagálni egy bekövetkező kibertámadásra,
- azt terv- és folyamatszerűen kezelni,
- az eseményt elszigetelni és felszámolni,
- csökkenteni az érintett, illetve függőség miatt kapcsolódó rendszer(ek)re gyakorolt hatást,
- a felszámolás után visszaállni az eredeti, üzemszerű állapotra.

Összefoglalás

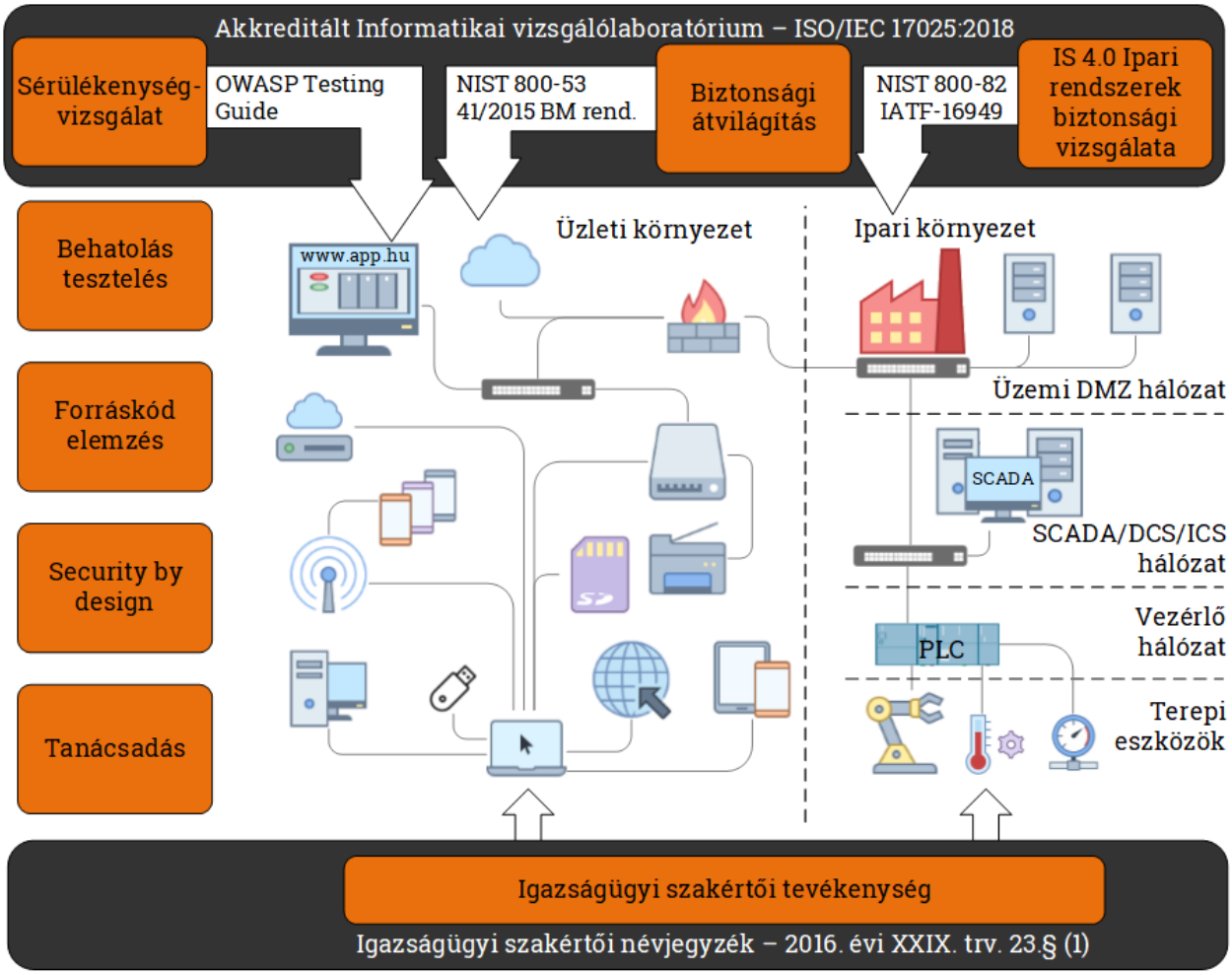
Látható, hogy a szabványmódosítás során beemelt kiberbiztonsági elvárásokkal kapcsolatban még akkor is lesznek tendői egy szervezetnek, ha azokkal már korábban is foglalkozott és kiépítette a megfelelő védelmet. Tanúsításkor ugyanis a fenti pontoknak való megfelelést objektív bizonyítékokkal kellhet alátámasztani.

Olyan esetekben, ahol az ipari kibervédelem korábban nem kapott hangsúlyt, vagy nem állnak rendelkezésre a szükséges eszközök, folyamatok és intézkedések, a megfelelőséghez jelentős erőforrásokra és szakértők bevonására is szükség lehet.

Bemutatkozik az Alverad

Az Alverad Technology Focus Kft. 2008-ban alapított, magyar tulajdonban lévő kiberbiztonsági vállalat, amely információvédelmi, informatikai és ipari kibervédelmi szakértői tevékenységgel foglalkozik.

Rendelkezünk informatikai és iparbiztonsági vizsgálólaboratóriummal, amelyet a Nemzeti Akkreditáló Hatóság (NAH) a nemzetközi ISO/IEC 17025:2018 szabvány szerint akkreditált, így munkánkat igazoltan és rendszeresen felülvizsgálva, megalapozott, szakmailag validált módszertanok mentén, folyamatosan képzett szakemberek végzik.



Szakértői tevékenységeink és szolgáltatásaink

Az Ipar 4.0 (és a már közelgő Ipar 5.0) igényei, az IoT, az ipari IoT , valamint a felhős rendszerekkel való kapcsolatok térhódítása miatt fontos küldetésünk, hogy segítsük partnereinket olyan rendszereket kiépíteni és működtetni, amelyek a változások és a növekvő fenyegetettségek mellett is biztonságosan üzemelnek, gyártanak és termelnek.

Az ipari rendszerek kibervédelme sok helyen jelentősen el van maradva az IT és irodai hálózatok védelmétől. Ennek oka a múltban keresendő, az ipari eszközök ugyanis korábban szigetszerűen működtek, nem volt igény olyan védelmi funkciók kialakítására, amelyek az IT és irodai rendszerek esetén általánosak és elvártak. Ezért az ipari eszközök hálózatba kötésével, a hálózatok összekapcsolásával olyan sebezhetőségek és kockázatok jelentek meg, amelyekkel a szervezeteknek ma már foglalkoznia kell. Erre mutat rá az IATF-16949 szabvány változása, és ebben szeretnénk mi is segítséget nyújtani partnereinknek!

Szolgáltatásaink IATF-16949 megfelelőséghez

Ipari kiberbiztonsági átvilágítás, kockázatfelmérés

Az autóipari minőségirányítási szabványnak megfelelni kívánt szervezetek részére nyújtott, az IATF-16949 megfelelőséget támogató felmérő és átvilágító szolgáltatásunkban megvizsgáljuk a szervezet rendszereit és folyamatait, hogy megfelelnek-e az általános ipari kibervédelmi, illetve a specifikus IATF-16949 szabvány kiberbiztonsági elvárásainak és elveinek.

A vizsgáló laboratóriumban, illetve a helyszínen elvégzett iparbiztonsági vizsgálatok a NIST SP 800-82 (revision 2), illetve a NIST SP 800-53 (revision 4) nemzetközi módszertani ajánlások alapján kerülnek megvalósításra. Az átvilágítás fókusza az IATF 16949 szabvány ipari kiberbiztonsággal kapcsolatos elvárásainak teljesülése, a megvalósítások módja és működése, valamint olyan hiányosságok, sérülékenységek és kockázatok feltárása, amelyek miatt a szabvány elvárásai esetlegesen nem teljesülnek, vagy amelyek miatt a megfelelőség nem igazolható.

Ipari és gyártási rendszerek sérülékenységvizsgálata

Magasan képzett, nemzetközi minősítéssel rendelkező etikus hackereink és ipari kibervédelmi szakértőink segítségével megvizsgáljuk a gyártási és termelési környezeteket, illetve a kapcsolódó vagy függőségi viszonyban lévő eszközöket és rendszereket.

Aktív vagy passzív sérülékenység-vizsgáló módszertanunk segítségével feltárásra kerülnek az eszközöket és rendszereket érintő műszaki és egyéb sérülékenységek, hiányosságok és gyengeségek, amelyek miatt a gyártási és termelési infrastruktúra esetlegesen sebezhető, és amelyek kihasználása fenyegetheti a működés és gyártás folyamatosságát.

A sérülékenységvizsgálati jelentés tartalmazza a feltárt sérülékenységeket, azok lehetséges hatásait, a feltárt sérülékenységek priorizálását és a sérülékenységek javítását célzó javaslatokat, valamint intézkedéseket.

ICS/OT biztonsági szabályzati környezet kialakítása

Sok esetben a vizsgált szervezet nem rendelkezik a specifikus, gyártási és termelési környezetek (OT), vagy az ipari irányító rendszerek (ICS) biztonsági szabályozását megvalósító eljárásrendekkel és szabályzatokkal.
Tapasztalt auditoraink segítségével felmérhetők a különféle rendszerek és termelési folyamatok, megállapíthatók a függőségek és kockázatok, valamint kialakításra kerülnek a vonatkozó specifikus, betartható és élhető biztonsági szabályok, amelyek nem akadályozzák a termelést, de jelentősen csökkentik és csillapítják a kockázatokat.

Minősítéseink

NAH-1-1829/2018
Vizsgálólaboratórium

A **Nemzeti Akkreditáló Hatóság** (NAH) akkreditált minket a Vizsgáló- és kalibrálólaboratóriumok felkészültségének általános követelményeit (ISO/IEC 17025:2017) tartalmazó, nemzetközi szabvány szerint. Ez azt jelenti, hogy **akkreditált informatikai és iparbiztonsági vizsgálólaboratórium**ként munkánkat igazoltan és rendszeresen felülvizsgálva, megalapozott, szakmailag validált módszertanok mentén, folyamatosan képzett szakemberek végzik.

IGAZSÁGÜGYI MINISZTÉRIUM

Az **Igazságügyi Minisztérium** társaságunkat bejegyezte az Igazságügyi Felügyeleti Főosztály által vezetett **igazságügyi szakértői névjegyzék**be, többek között számítástechnikai adatbázis, adatstruktúrák, szoftverek, informatikai rendszerek, berendezések és informatikai biztonság szakterületekkel. Ezzel jogosulttá váltunk olyan szakvélemények kiadására, melyek akár hatósági vagy büntető eljárásokban is felhasználhatóak.

NEMZETI BIZTONSÁGI FELÜGYELET

A **Nemzeti Biztonsági Felügyelet** a minősített adat védelméről szóló 2009. évi CLV. törvény 16.§-ában, valamint az iparbiztonsági ellenőrzés és a telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III.31.) Korm. rendelet 6. §-ban foglaltakkal összhangban **szigorúan titkos** szintű egyszerűsített **telephely biztonsági tanúsítvány**t adott ki vállalatunk részére. Ez azt jelenti, hogy cégünk és a munkatársaink nemzetbiztonsági átvilágításban részesültek, dolgozhatnak minősített projekteken, azaz megvalósítják a diszkréció azon fokát, amely mellett akár államtitkok megismerésére is jogosulttá válhatnak.

1990 A haza minden előtt ALKOTMÁNYVÉDELMI HIVATAL

Az **Alkotmányvédelmi Hivatal** Iparbiztonsági Osztálya a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló **271/2018. (XII. 20.) Korm. rendelet** 22. § (5) bekezdése alapján vezetett **nyilvántartás**ba Vállalatunkat felvette. Ezzel jogosulttá váltunk bizonyos állami intézmények, hivatalok rendszereinek külső informatikai biztonsági vizsgálatára, webes vizsgálatára, belső informatikai biztonsági vizsgálatára, illetve vezeték nélküli hálózat informatikai biztonsági vizsgálatára. Továbbá felvételt nyertünk a védelmi és biztonsági célú beszerzésekről szóló **2016. évi XXX. törvény** 116. § (1) bekezdése alapján vezetett **nyilvántartás**ba is. Ez lehetőséget biztosít számunkra a védelmi és biztonsági célú beszerzéseken történő ajánlattételre, illetve minősített adatokat érintő projektekben való részvételre.

MSZ EN ISO 9001:2015 szabvány szerinti minőségirányítás

MSZ EN ISO/IEC 27001:2014 szabvány szerinti információ biztonság