QTICS GROUP

PROFESSIONAL.INTELLIGENT.HUMAN

A kiberbiztonság szerepe az orvostechnikában

Arató György

Miről lesz szó?

- Információbiztonság
- Kiberbiztonság
- Cybersecurity Act
- Orvostechnikában a kiberbiztonság

Információbiztonság

az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben használt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázattal arányos

Kiberbiztonság

a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalom és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.

Cybersecurity Act

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az ENISA-ról, az „Európai Uniós Kiberbiztonsági Ügynökségről”, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról („kiberbiztonsági jogszabály”)

„A bizalom és biztonság megteremtése és megőrzése érdekében az IKT termékekbe és -szolgáltatásokba már a műszaki tervezés és fejlesztés korai szakaszaiban közvetlenül be kell építeni a biztonsági elemeket (beépített biztonság). Továbbá a vásárlóknak és felhasználóknak meg kell tudniuk állapítani az általuk beszerzett vagy megvásárolt termékek és szolgáltatások biztonsági szintjét.”

„A jelenlegi javaslat meghatározza az európai kiberbiztonsági tanúsítási rendszerekre vonatkozó szabályok átfogó keretrendszerét.”

Kiberbiztonság az orvostechnikában

MDR / IVDR I. melléklet II. fejezet, 17.2 bekezdés

17.2. Szoftvert tartalmazó eszközök vagy az önmagukban eszköznek minősülő szoftverek esetében a szoftvert a technika állásának megfelelően, a fejlesztés életciklusára, **a kockázatkezelésre – az információbiztonságot is beleértve** –, az ellenőrzésre és a validálásra vonatkozó elveket figyelembe véve kell fejleszteni és gyártani.

Kiberbiztonság az orvostechnikában

MDR / IVDR I. melléklet II. fejezet, 17.2 bekezdés

17.4. A gyártóknak a szoftver rendeltetésszerű üzemeltetéséhez szükséges minimumkövetelményeket kell meghatározniuk a hardverre, az **információtechnológiai hálózatok jellemzőire és az információtechnológiai biztonságot célzó intézkedésekre** vonatkozóan, **beleértve a jogosulatlan hozzáférés elleni védelmet is.**

Kiberbiztonság az orvostechnikában

MDR / IVDR I. melléklet II. fejezet, 18.8 bekezdés

18.8. Az eszközök kialakításának és gyártásának olyannak kell lennie, hogy a lehető legnagyobb mértékű védelmet lehessen biztosítani az eszközökhöz való olyan **jogosulatlan hozzáféréssel szemben, amely gátolhatja az eszközök rendeltetésszerű működését.** !

Orvostechnikában a kiberbiztonság

- Vállalati biztonság növelése (pl.: ISO 27001)
- Security by desing! – Már akkor gondolni kell a biztonságra, amikor még csak tervezzük a terméket.
- Fejlesztés során is folyamatosan biztonságosan kell fejleszteni a terméket.
- Kiadás során biztonsági tesztelést kell végrehajtani.
- Kiadást követően is folyamatosan figyelni kell a sérülékenységeket.

Orvostechnikában a kiberbiztonság

Threat modeling – Fenyegetés modellezés

A fenyegetés modellezésének célja, hogy a védelemi szempontból szisztematikus elemzést nyújtson arról, hogy milyen kontrollokat vagy védelmeket kell tartalmaznia az adott eszköznek, tekintettel a rendszer jellegére, a valószínű támadó profiljára, a legvalószínűbb támadási vektorokra és a támadó által leginkább kívánt eszközökre.

„Hol vagyok a leginkább kiszolgáltatott a támadásnak?”
„Melyek a legrelevánsabb fenyegetések?”
„Mit kell tennem, hogy elhárítsam ezeket a fenyegetéseket?”

Threat mitigation testing –
Fenyegetettség mérséklésének tesztelése

A kiberbiztonsági fenyegetések mérséklése a vállalatok által bevezetett irányelvekre és folyamatokra vonatkozik, amelyek segítenek megelőzni a biztonsági eseményeket és az adatok megsértését, valamint korlátozzák a kár mértékét.

Minden ilyen intézkedésre tervet kell alkotni, és ezeket vizsgálni kell, hogy az intézkedés megfelelően hatékony és ezeket vissza kell ellenőrizni (tesztelni).

Vulnerability testing –
Sérülékenység vizsgálat

A sebezhetőségi értékelésnek is nevezett biztonsági rés-teszt a rendszerek biztonsági kockázatainak értékelése a fenyegetések valószínűségének kiküszöbölése érdekében.

A tesztelés célja annak megakadályozása, hogy a behatolók / hackerek jogosulatlanul hozzáférjenek a rendszerekhez.

A biztonsági rés minden olyan hiba vagy gyengeség a rendszer biztonsági eljárásaiban, tervezésében, megvalósításában vagy bármilyen belső ellenőrzésben, amely a rendszer biztonsági házirendjének, működésének megsértését eredményezheti.

Összegezve

A fejlesztés teljes életciklusában meg kell, hogy jelenjen a biztonságtudatosság.

Vállalati biztonsági folyamatokat ki kell alakítani és tesztelni kell.

A termék tervezése során nem csak a funkcionális és nem funkcionális területekre kell koncentrálni, hanem a biztonsági elemekre is.

A fejlesztés során egy-egy fázisban vizsgálni kell a termékben a biztonságos folyamatokat, részeket.

Termék kiadása során külön biztonsági tesztelést kell alkalmazni.

www.qtics.group

medical