ÚTMUTATÓ A BORZASZTÓ INFORMÁCIÓBIZTONSÁGHOZ

Az ebben a dokumentumban található gyakori hibák megismerésével könnyebbé válik elkerülésük.

Biztonsági házirend és *Compliance*

Ne vedd figyelembe a *compliance* követelményeket!

Feltételezd, hogy a felhasználók puszta kérésedre elolvassák a biztonsági házirendet!

Használj biztonsági sablonokat testreszabás nélkül!

Ess neki keretrendszerek, mint az ISO 27001/27002 teljes bevezetésének megfelelő érettség előtt!

Készíts betarthatatlan biztonsági házirendet!

Tartass be el nem fogadott házirendet!

Kövesd vakon a *compliance* követelményeket általános biztonsági architektúra létrehozása nélkül!

Írj biztonsági házirendet, csak hogy kipipálhasd ezt is!

Fizess valakit meg, hogy megírja a biztonsági házirendet céged vagy folyamatainak ismerete nélkül!

Többnyelvű környezetben az előírások fordításánál felesleges az egyes nyelvek közti konzisztencia.

Nehogy megtalálják az alkalmazottak a házirendet!

Nyugodtan feltételezd, hogy a tavaly sikeresen alkalmazott házirend idén is ugyanúgy érvényes lesz!

Ha *compliant* vagy, akkor biztonságban vagy.

A házirend nem vonatkozik felsővezetőkre.

Bújj el az auditorok elől!

Biztonsági eszközök

A biztonsági eszközöket finomhangolás nélkül üzemeld be, ahogy a dobozból kijött, úgy tökéletes!

Az IDS legyen túl hangos vagy túl halk!

Vásárolj biztonsági termékeket karbantartási és bevezetési költségek figyelembevétele nélkül!

Bízz mindent az antivírus és tűzfal termékekre, további kontrollok bevezetése felesleges!

Futtass rendszeres sérülékenység-felderítést, de a kimenetet hagyd figyelmen kívül!

Az antivírus, IDS és egyéb biztonsági eszközök mehetnek „robotpilótával”.

Alkalmazz többféle biztonsági technológiát az egyes elemek szerepének átgondolása nélkül!

Fókuszálj a diagramokra, figyelmen kívül hagyva a felelősség folytonosságának a fontosságát!

Vásárolj drága termékeket akkor is, ha egy egyszerű és olcsó módon megoldható a probléma 80%-a!

Kockázatmenedzsment

Próbáld meg ugyanazt a szigort alkalmazni minden IT eszközre, függetlenül annak kockázati besorolásától!

Tegyél valakit felelőssé a kockázatmenedzsmentért, döntési jogkört viszont nehogy adj neki!

Hagyd figyelmen kívül a teljes képet, amikor épp kvantitatív kockázatmenedzsmenttel foglalkozol!

Nyugodtan feltételezd, hogy nem kell aggódnod a biztonságon, mivel a cég túl kicsi vagy jelentéktelen!

Nyugodtan érezd a céget biztonságban, mivel az utóbbi időben nem történt kompromittáció nálatok!

Legyél paranoiás a védendő adat vagy rendszerelem értékétől és kitettségétől függetlenül!

Az összes adatot nyilvánítsd „szigorúan titkosnak”!

Biztonsági gyakorlat

Ne nézegesd a rendszer-, alkalmazás- és biztonsági naplókat!

A felhasználóktól elvárhatod, hogy a kényelmet feladják a biztonságért.

Bástyázd körül annyira az infrastruktúrát, hogy nagyon nehéz legyen bármilyen munkát elvégezni!

Kérések elbírálásánál mindig mondj nemet!

Írj biztonsági követelményeket a betartáshoz szükséges eszközök és oktatás biztosítása nélkül.

Fókuszálj a preventív mechanizmusokra, az utólagos detektálást szolgáló kontrollok nem érdekesek!

Ne legyen DMZ az Internet felé néző szervereknek!

Nyugodtan feltételezd, hogy a patch menedzsment folyamatod működik, felesleges ellenőrizni!

Töröld a naplókat, mert túl nagyok az olvasgatáshoz!

Várd az SSL-től a megváltást a webalkalmazásodat érintő összes biztonsági problémára!

Tiltsad be a pendrive-ok használatát, miközben az Internet felé menő forgalom korlátlanul folyhat!

Viselkedj felsőbbrendűként a hálózati, rendszergazdai és fejlesztői csapatokbeli kollégákkal!

Felesleges tanulni új technológiáról és támadásokról.

Vegyél át új és menő IT vagy biztonsági technológiákat mielőtt lehetőségük lenne érettebbé válni!

Új kollégák felvételekor kizárólag a minősítések számát vedd figyelembe!

Ne értesítsd a főnöködet az erőfeszítéseid kapcsán elkerült biztonsági problémákról!

Ne legyen kereszt-tréning IT és biztonsági csapatnak!

Jelszómenedzsment

Követeld meg a felhasználóktól a túl gyakori jelszóváltást!

Várd el a felhasználóktól, hogy megjegyezzék a jelszavakat anélkül, hogy leírnák azokat!

Kényszeríts ki túlzottan szigorú jelszóválasztási követelményeket!

Használj egyező jelszavakat különböző kockázati kitettségű és biztonsági besorolású rendszereken!

A jelszó-követelmények megalkotásakor hagyd figyelmen kívül a jelszó-visszaállítás bonyolultságát!

További biztonsági botlások (angolul)

The 10 Dumbest Things People Do...
http://www.sans.org/newsletters/ouch...

10 common security mistakes...
http://www.techrepublic.com/blog/10-things...

Mistakes ... that Lead to Security Breaches
http://sans.org/resources/mistakes.php?ref=3816

Írta Lenny Zeltser, a SANS Internet Storm Center szakértő munkatársainak kiegészítéseivel. Magyarra fordította a Silent Signal csapata, akik szakmai tapasztalataikat (részben a fentiekről) rendszeresen megosztják angol nyelvű techblogjukon (https://blog.silentsignal.eu/). A Creative Commons v3 “Attribution” Licensz vonatkozik a fenti listára, melynek az az 1.3-as verziója.