Kihívások mellett lehetőséget is tartogat a NIS2 a magyar cégeknek

A NIS2 irányelv új követelményei nagyon sok szereplőt érintenek a magyar vállalati ökoszisztémában, hiszen a kockázatos ágazatokon túl közvetve ezen ágazatok beszállítóira is hatással vannak – hangzott el a CETIN Hungary IVSZ-szel közösen rendezett, teltházas rendezvényén. A kiberbiztonsági előírásokat be nem tartó cég súlyos következményekkel számolhat: a büntetés mértéke az éves árbevétel 2 százalékát is elérheti. A NIS2 ugyanakkor nem csupán egy újabb szabályozás, hanem olyan eszköz, amely versenyelőnnyé is formálhatja a kiberbiztonsági megfelelést.

A 2016-ban bevezetett európai uniós kiberbiztonsági szabályokat a 2023-ban hatályba lépett NIS2 irányelv aktualizálta annak érdekében, hogy lépést tartson a digitalizációval és a folyamatosan változó kiberbiztonsági fenyegetésekkel. Az irányelv új ágazatokra és szervezetekre terjeszti ki a kiberbiztonsági szabályok hatályát. Magyarországon az idén januárban hatályba lépett, kiberbiztonsági tanúsításról és kiberbiztonsági felügyeletről szóló törvény ültette át a hazai jogrendbe a NIS2-t.

Október 18-án fontos mérföldkőhöz értünk: az érintett szervezetek innentől kezdődően kell megfeleljenek a törvény előírásainak. Dr. Bencsik Balázs, a Szabályozott Tevékenységek Felügyeleti Hatósága részéről kiemelte: a NIS2 irányelv által támasztott új követelmények ez után komolyabb kötelezettségeket jelentenek a magyar vállalkozások számára. Az irányelv a kiberbiztonsági szabályozást az egyre komplexebb digitális fenyegetésekhez igazítja, és különös figyelmet fordít azokra a kockázatos ágazatokban működő vállalatokra, amelyek legalább 50 főt foglalkoztatnak, vagy éves árbevételük meghaladja a 10 millió eurót.

A NIS2 előírások be nem tartása esetén súlyos következményekkel számolhat egy cég, hiszen a büntetés mértéke az éves árbevétel 2%-át is elérheti.

Dr. Bencsik Balázs kitért az auditálás folyamatára is, amely a vállalati informatikai rendszerek biztonsági osztályba sorolásával kezdődik, és számos vizsgálatot, köztük sérülékenységi és behatolásvizsgálatot is magába foglal. A hatóság a szervezetek értékelésére új mutatót vezet be: a védelmi megfelelőségi és a szervezeti ellenállóképességi indexből képzett mérőszám olyan mutató lesz a kiberbiztonsági auditot sikerrel teljesítő vállalatoknak, ami üzleti partnereik szemében is előnyös képet fest majd róluk.

Összességében fontos kiemelni, hogy bár az EU-s irányelvvel kapcsolatos feladatok jelentős kihívást jelentenek, a magyar vállalatok eddigi hozzáállása – az SZTFH tapasztalatai alapján – pozitív képet mutat, ami biztató jel a jövőbeni megfelelés szempontjából.

Weisz Csaba, a CETIN Hungary senior biztonsági tanácsadója hangsúlyozta: a NIS2 irányelv új, szigorított követelményei immár a kockázatos ágazatokban működő szervezetek beszállítóira is hatással van – így akár kisebb vállalkozásoknak is alkalmazkodniuk kell a szigorú elvárásokhoz, ami számukra teljesen új kihívást jelent. A megfelelés elkerülhetetlenül egyfajta kultúraváltáshoz is fog vezetni, az audit sikerét tapasztalt szakértők segíthetik elő. A partneri ökoszisztéma tagjai – a hatóságok, a NIS2 megfelelőségre kötelezett cégek és beszállítóik – közötti együttműködés kulcsfontosságú a NIS2-ben megfogalmazott célok eléréséhez. A CETIN számos auditot sikeresen teljesített, így megvan az a tapasztalata, amellyel segíteni tudja azokat a partnereit és beszállítóit, akik még nem vettek részt ilyen komplexitású auditokon.

A szakember előadása végén arra biztatta a jelenlévő cégek képviselőit, hogy a NIS2 előírásait ne

csupán kötelezettségként, hanem lehetőségként kezeljék, ami a jövőbeni üzleti sikerük fontos összetevője lehet.

Matek Kamilló, a KPMG Cyberlab vezetője, etikus hacker egy valós hackertámadás részleteinek feltárásával világított rá a folyamatos biztonsági tesztelések jelentőségére. A legtöbb sérülékenységvizsgálat során a cégek általában csak technológiai rendszereket vagy felhasználói tudatosságot tesztelnek, míg a folyamatok, a rendszerek és az emberi tényezők együttes vizsgálata gyakran elmarad.

Az előadás során a szakember egy ügyfélnél végrehajtott ún. Red Teaming gyakorlatot ismertetett, ahol sikeresen kihasználta a vállalat rendszerében egy DLP szoftver részeként jelen lévő Python komponenst. A régi megoldást alkalmazó elem sérülékenységeit és beállításait kihasználva az etikus hacker a Microsoft védelmi rendszerét is megkerülve social engineering támadást hajtott végre, és sikeresen távoli hozzáférést szerzett a társaság rendszereihez anélkül, hogy a védelmi mechanizmusok erről riasztást adtak volna.

Matek Kamilló hangsúlyozta, hogy a hagyományos biztonsági tesztek gyakran nem derítik fel ezeket a mélyen megbúvó sebezhetőségeket, ezért szükség lehet olyan biztonsági tesztelésekre, amelyek a maguk teljességében, valós körülmények között vizsgálják a cég rendszereit. Ezek a gyakorlatok nem csupán a nagyvállalatok, hanem kisebb cégek számára is elengedhetetlenek a valódi biztonság megteremtéséhez.

Sajtókapcsolat:

- Hegedüs Bertalan, ügyfélmenedzser
- NOGUCHI
- bhegedus@noguchi.hu

© CETIN Hungary
Matek Kamilló, KPMG Cyberlab vezető, etikus hacker.

© CETIN Hungary
Dr. Bencsik Balázs, Szabályozott Tevékenységek Felügyeleti Hatósága.

© CETIN Hungary
Weisz Csaba, senior biztonsági tanácsadó, CETIN Hungary.

Eredeti tartalom: CETIN Hungary

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el:
https://hellosajto.hu/16407/kihivasok-mellett-lehetoseget-is-tartogat-a-nis2-a-magyar-cegeknek/