KOVÁCS RÉTI SZEGHEŐ
ÜGYVÉDI IRODA

A GDPR-t már mindenki ismeri…de a NIS-t is?

Már az ovisok is tudják álmukból felkeltve is, hogy mit jelent a GDPR mozaikszó, de az ún. NIS irányelvről nem nagyon hallani. Pedig, a kiberbiztonsági szabályozásnak egy fontos eleme, és az előírásainak történő nem megfelelés ugyanúgy jogkövetkezményekkel jár, mint a GDPR szabályainak nem betartása.

De mi is az a NIS?

Az Európai Parlament és a Tanács 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről **(„NIS irányelv")**. Célja annak biztosítása, hogy az uniós országok jól felkészültek legyenek az európai infrastruktúra elleni kibertámadásokra, készen álljanak azok kezelésére, illetve az azokra való hatékony reagálásra. A NIS irányelvet az Európai Parlament 2016. július 6. napján hagyta jóvá, és 2016. augusztus 8-án lépett hatályba.

A NIS irányelv - mint uniós szintű szabályozás - megalkotása azért volt szükséges, mert egyfelől a kibertámadások száma évről-évre növekszik, másfelől egy-egy hálózat- vagy információbiztonsági incidens az egész Unióra is kihathat. Az idei 2019-es évben a korábbiakhoz képest még nagyobb adatlopási incidensek, illegális rendszer- és hálózatfeltörések várhatóak. Magyarországon például a PSD II irányelvhez kapcsolódóan 2019. július 1-jén elindul az azonnali fizetési rendszer, amelynek keretében a hazai pénzintézeteknek a hét minden napján, 0-24 óráig 5 másodpercen belül teljesíteniük kell az átutalásokat. Ezzel párhuzamosan szignifikánsan növekedni fognak a banki ügyfelek elleni adathalász támadások, valamint az ügyfelek számítógépjeire és mobil eszközeire feltelepülő ún. bankoló trójai szoftverek fertőzései.

Átfedések és eltérések a GDPR és NIS irányelv között

A GDPR minden olyan szervezetre vonatkozik, amelyik európai állampolgárok személyes adatait kezeli, a NIS csak azokra a szolgáltatókra, amelyeknek a megtámadása a legérzékenyebben érinti a társadalmat. A NIS által érintett egyik csoport az **alapvető szolgáltatást nyújtó szolgáltatók** (pl. egészségügyi szolgáltatók, bankok, energiacégek, ivóvízellátók, közlekedési vállalatok), a másik **azon digitális szolgáltatásokat nyújtó szolgáltatók**, amelyek ugyan nem nélkülözhetetlen, de fontos társadalmi hatású szolgáltatásokat kínálnak (**keresőszolgáltatások, online piacterek és a felhőszolgáltatók).** Mindkét csoport esetében is csak olyan szolgáltatásokra vonatkozik, amelyek rendellenes működése vagy kiesése komoly társadalmi vagy gazdasági károkat okozna. Például nyilvánvalóan ide tartozik, ha egy bank online szolgáltatásait támadják, ellenben már nem tartozik ide, ha kizárólag a bank marketing részlege érintett egy kibertámadás által.

Mind a GDPR, mind a NIS érinti nem csak az Unión belül, de azon kívül letelepedett szolgáltatókat is, amennyiben az EU területén szolgáltatást nyújtanak. Ennek megfelelően érintettnek minősöl például az USA székhelyű Google és Amazon, ezen kívül az EU-n belül működő brit cégeknek a brexit után is meg kell felelniük majd ezen jogszabályoknak.

A GDPR közvetlenül alkalmazandó joganyag, ezzel szemben a NIS Irányelvet a tagállamoknak implementálniuk kell a belső jogukba. A NIS irányelvet a magyar jogba átültető jogszabályok közül kiemelnénk az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvényt, valamint az információs

társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló 270/2018. (XII. 20.) Kormányrendeletet.

Mindkét szabályozás bejelentési kötelezettséget ír elő bizonyos incidensek esetén. Eltérés van azonban a bejelentési kötelezettséget megalapozó esemény tekintetében és abban, hogy ki felé kell a bejelentést megtenni.

A GDPR alapján az adatvédelmi incidenseket (azaz a személyes adatokat érintő incidenseket) be kell jelenteni a Nemzeti Adatvédelmi és Információszabadság Hatóságnak (NAIH), továbbá az incidenssel érintett jogalany köteles az adat tulajdonosát, vagyis a felhasználót is értesíteni. A NIS Irányelv alapján az ún. „biztonsági eseményeket" (azaz minden olyan eseményt, amely ténylegesen kedvezőtlen hatást gyakorol a hálózati és információs rendszerek biztonságára) kell bejelenteni; a bejelentési kötelezettség kizárólag a Nemzetbiztonsági Szakszolgálat (NBSZ) irányában áll fenn.

Az előírásoknak meg nem felelés jogkövetkezményei

Közismert, hogy a GDPR előírásainak meg nem felelés esetén a kiszabható bírság maximális mértéke 20 millió euró, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4%-át kitevő összeg. A NIS irányelvet implementáló 270/2018. (XII. 20.) Kormányrendeletet **alapján a kiszabható bírság maximuma ötmillió forint, de egy-egy incidens kettős, a GDPR és a NIS irányelv szerinti szankciókat is eredményezhet. Az említett igazgatási jogkövetkezmények mellett az érintetteknek polgári jogi jogkövetkezményekkel is számolniuk kell**. Kiberbiztonsági események nyomán sor kerülhet értékpapírokkal kapcsolatos és fogyasztói csoportperekre, ezen kívül súlyos felelősségbiztosítási következményekkel is járhat, ha a károsult adatalany kártérítési követeléssel lép fel.