Nem a digitális világhoz készültek a kritikus infrastruktúrák

Az áram-, energia- és vízhálózatokat, továbbá más rendszereket nehéz felkészíteni a 21. század kihívásaira.

A Vienna Cyber Security Week 2019 nevű rendezvény keretében a szakértők arról tanácskoztak, hogy a kritikus infrastruktúrákat hogyan lehetne megvédeni a kibertámadásokkal szemben. *Donald Dudenhoeffer*, az EnergyPact Foundation ügyvezetője és az Osztrák Technológiai Intézet (AIT) kiberbiztonsági kutatómérnöke kijelentette, hogy az energiaszektor műszaki rendszereit még egy analóg időszakban fejlesztették ki. Ugyan most megpróbálják azokat digitalizálni, így sokkal bonyolultabbá válnak, viszont ezáltal nőnek egy ellenük irányuló kibertámadás kockázatai is.

Esti Peshin, az Israel Aerospace Industries Ltd. (IAI) kiberrészlegének ügyvezetője kiemelte, hogy nem csupán az energiaszektor, hanem a szállítási ágazat, az egészségügyi rendszer és a légi közlekedés is számos olyan rendszerrel van ellátva, amelyek a mai követelmények szempontjából teljesen elavultnak számítanak. Ezeket a meglévő analóg rendszereket ugyan folyamatosan digitalizálják, de ennek ellenére sincsenek a kiberbiztonságra felkészítve, így a védettségük biztosítása komoly kihívást jelent.

A menedzser hozzátette, hogy a növekvő hálózatba kötöttség nem igazán teszi egyszerűbbé a biztonsági szakemberek munkáját. A dolgok internete rendszerek rendkívül nagy kockázatot jelentenek, mert gyakran nem megfelelő módon védik azokat és számos támadási felületet kínálnak. Amennyiben valaki egyszer sikeresen megfertőzte egy dolgok internete infrastruktúrában a főhálózatot, utána a kártevőt automatikusan továbbítódik az összes csatlakoztatott készülékre.

Az IAI szakértője szerint a megoldás egy olyan technikai felszerelés lenne, amely korszerű és megfelel a legújabb követelményeknek. Emellett fontos, hogy az IT-biztonság területén soha nem dőlhetnek hátra a kutatók, s folyamatosan új ötleteket és lehetőségeket kell keresniük. Szintén fontos az összes érdekelt féllel való együttműködés. Elkerülhetetlenek továbbá az állandó tréningek és a munkatársak képzése is. Az „ottfelejtett” USB-kulcsok, az adathalász levelek, a hamis frissítések és a nem biztonságos magán eszközök még mindig hatékony beszivárgási módszereknek számítanak. Ahogy Peshin megfogalmazta: „Jelenleg és a jövőben is az ember a leggyengébb láncszem.”

Forrás: https://sg.hu/cikkek/it-tech/135595/nem-a-digitalis-vilaghoz-keszultek-a-kritikus-infrastrukturak

Válogatta: Berke Barnabásné