ISACA MÁSODIK SZERDAI ELŐADÁS

Sándor Barnabás

Mennyire biztonságos egy okosotthon?

2022.10.12.

ISACA
Budapest Chapter

FELELŐSSÉG KIZÁRÁSA

Az elhangzott prezentációk tartalmát illetően az ISACA Magyarországi Egyesület nem vállal felelősséget az abban nyújtott információk aktualitásáért, helyességéért és teljességéért.

Az itt elhangzott információk nem feltétlenül egyeznek meg az ISACA Magyarországi Egyesület álláspontjával.

ISACA® Budapest Chapter

Bevezető

Téma aktualitása

- Folyamatos technológiai fejlődés és automatizálás;
- Kényelmes, energiatakarékos és hatékony társadalom;
- Állandó online jelenlét;
- Elérhető áru okos eszközök.

ISACA Budapest Chapter

Alapvetések

Okosotthonok kiberbiztonságának vizsgálata

- IoT eszközök sebezhetőségei;
- A biztonság leggyengébb láncszeme az ember;
- Vezeték nélküli kommunikáció sérülékenységei.

ISACA®
Budapest Chapter

Okosotthon koncepció

- Könnyebbé, biztonságosabbá és környezettudatosabbá teszi életünket;
- Megfigyeli a szokásainkat;
- Illeszkedik a napi rutinunkhoz;
- Beavatkozás nélkül működik.

ISACA Budapest Chapter

Okosotthon funkciók

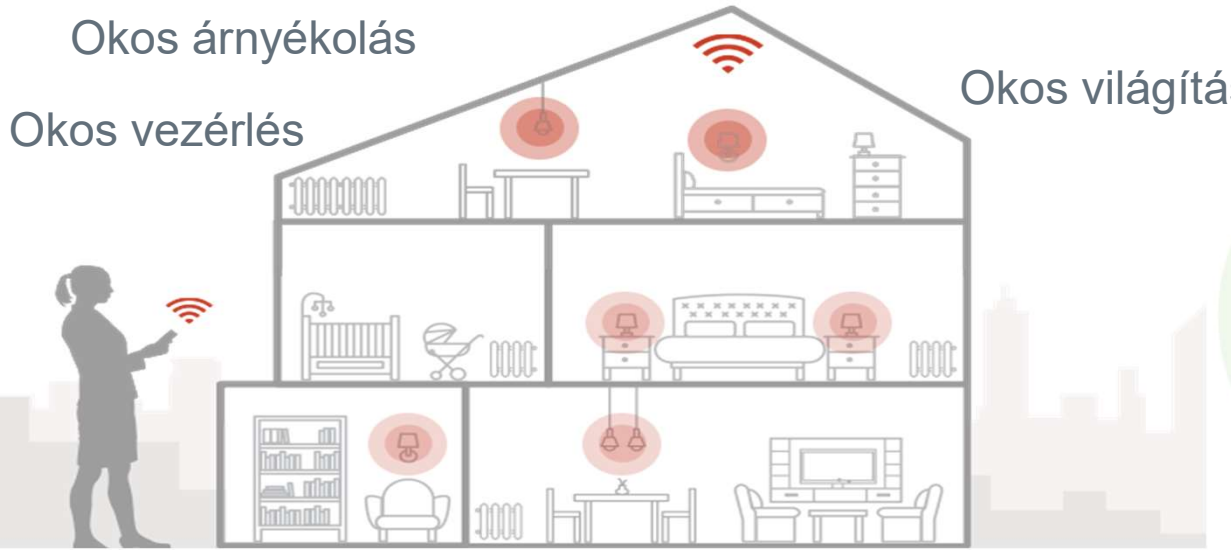
Okos biztonság

Okos hűtés/fűtés

Okos árnyékolás

Okos világítás

Okos vezérlés



Okos kertészkedés

ISACA Budapest Chapter

A dolgok internete

Internet of Things, avagy a Dolgok Internete

- “Intelligens tárgyak”, melyek egymással kommunikálnak;
- Beavatkozás nélküli kommunikáció és működés;
- Folyamatos adatgyűjtés és monitorozás;
- Üzleti döntések segítése és gyorsítása;
- Egybekapcsolt hálózat.

ISACA
Budapest Chapter

IoT eszközök

- Google, Amazon, Apple Home
- Kapucsengő, kamera
- Világításvezérlő, okos dugalj, izzó
- TV, multimédia eszközök
- Légtisztító, klíma, kazán
- Robot porszívó, mosógép
- Fogyasztásmérés

ISACA®
Budapest Chapter

Kiberbiztonsági fenyegetések

Kiberbiztonság

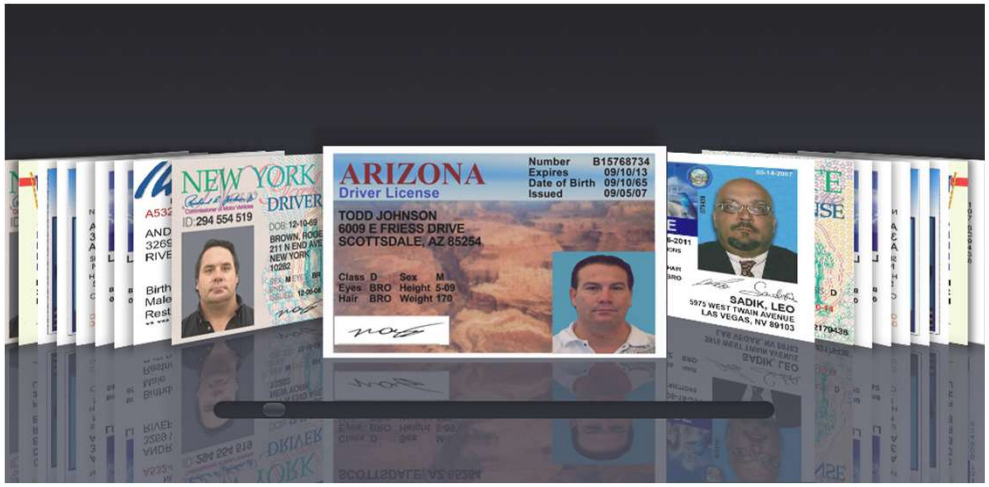
- Sérülékeny eszközök, szoftverek;
- Nem megfelelően telepített és konfigurált rendszer;
- Bizonytalan forrásból származó eszköz, szoftver;
- Alacsony szintű titkosítás;
- Célzott hacker támadások;
- Kampányszerű hacker támadások.

ISACA Budapest Chapter

Kiberbiztonsági fenyegetések

Adat-, és információbiztonság

- Adatokhoz való hozzáférés;
- Adatokkal való visszaélés.



ISACA®
Budapest Chapter

Kiberbiztonsági fenyegetések

Felderítés, célzott támadás

- Célzott felderítés és támadás az IoT protokollok ellen;
- Z-wave, WiFi, Bluetooth, ZigBee, MQTT, Sigfox, LoRaWAN, NFC, cellular.

ISACA Budapest Chapter

Kiberbiztonsági fenyegetések

R4IoT – Ransomware for IoT

- Vedere Labs által fejlesztett és tesztelt támadási mód;
- IT, OT és IoT rendszerek ellen összehangolt támadás;
- Már nem a titkosításról, hanem a valós zsarolásról szól.

ISACA
Budapest Chapter

Kiberbiztonsági fenyegetések

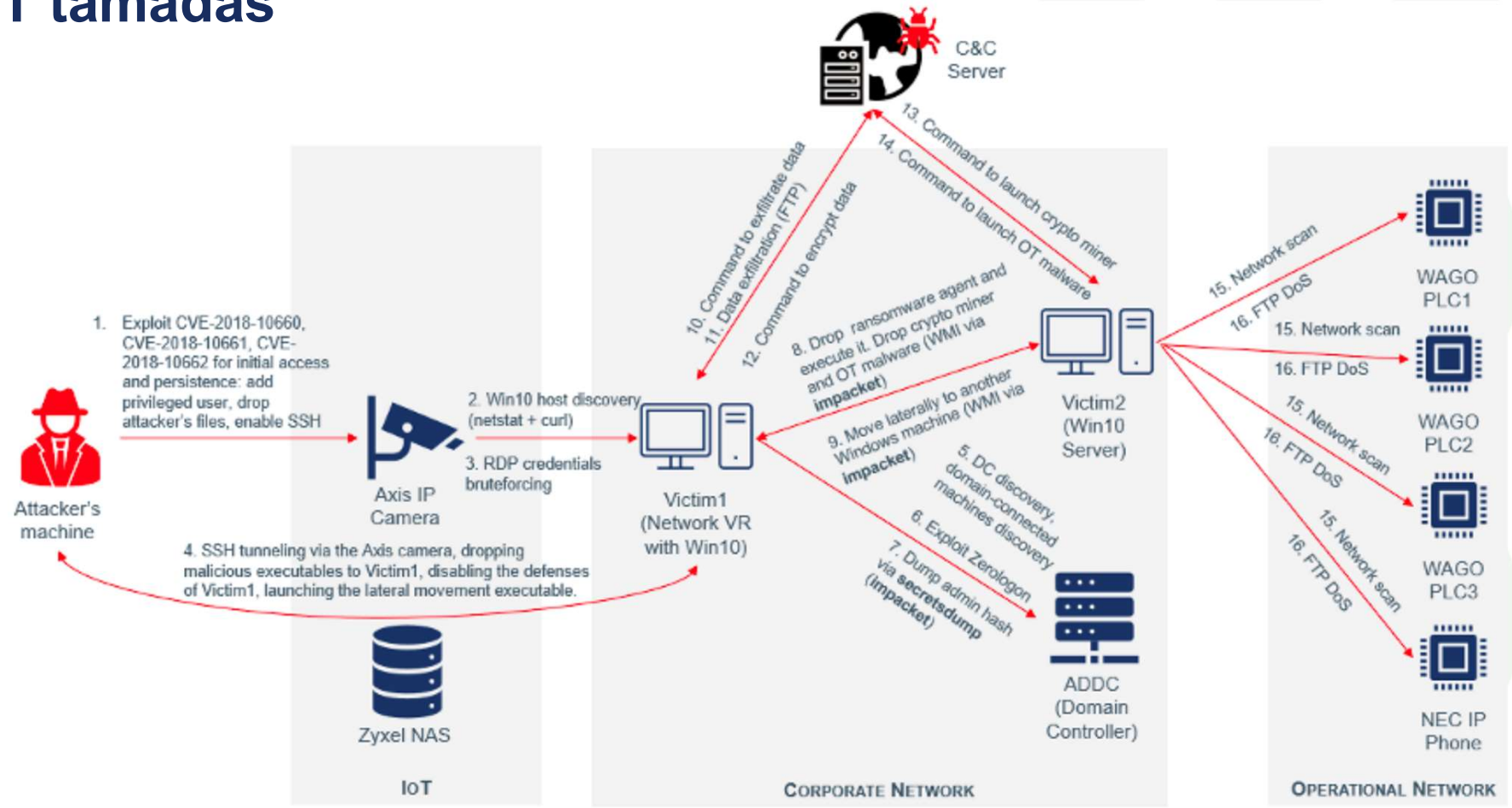
Ransomware támadás alapvetése

- Kezdeti sérülékenységgel hálózati hozzáférés (0-day, missconfig, etc);
- További terjeszkedés (2021. 90%-ban RDP);
- Adatgyűjtés, további fertőzés C2.

Figure 1 – High-level Anatomy of a Ransomware Attack

ISACA Budapest Chapter

R4IoT támadás



ISACA Budapest Chapter

Gyakorlati bemutató

SHODAN

ISACA®
Budapest Chapter

Megelőzési javaslatok

- Megbízható eszköz, telepítő kiválasztása;
- Megfelelő jelszó-, és jogosultságkezelés;
- Firmware, szoftver folyamatos frissítése;
- Hálózati szeparáció (DMZ, VLAN, WiFi);
- Tűzfal szabályok;
- VPN kapcsolat;
- Nyitott portok ellenőrzése.

ISACA®
Budapest Chapter

Sándor Barnabás

- sandor.barnabas@snb.hu
- www.sandorbarnabas.hu

sandorbarnabas

ISACA®
Budapest Chapter

KÖSZÖNÖM A FIGYELMET!

ISACA®
Budapest Chapter