Защита на крайните устройства от кибератаки

INFOSEC & DATA STORAGE

гр. София, 28.9.2017 г.

Здравко Стойчев, CISM CRISC

Societe Generale Експресбанк

ICT Media

ISACA Serving IT Governance Professionals Sofia Chapter

Кибер сигурност?

Кибер-атака се определя като всякакъв вид офанзивно действие от страна на държави, отделни лица, групи или организации, насочено към компютърни информационни системи, инфраструктура, мрежи или персонални компютърни устройства чрез различни средства за злоумишлени действия, обикновено произхождащо от анонимни източници, с цел кражба, промяна или унищожаване на определена цел чрез нахлуване в податлива система. Примери:

- **Вируси** – само-репликираща се програма, която се прикрепя към друга програма или файл, за да се възпроизведе
- **Червеи** – самостоятелна програма, която се разпространява в компютърна мрежа
- **Троянски кон** – злонамерен код, вграден в законна програма

Кибер сигурност – Факти

- 1млн професионалисти по кибер сигурност са в недостик в световен мащаб.[1]
- 86% смятат, че има липса на добре обучени професионалисти по кибер сигурност.[2]
- 82% са претърпели кибер заплаха или пробив през последните 12 месеца.[3]
- 83% от организациите имат недостиг на умения, нужни за защитата на техните ИТ активи.[2]

1) Cisco'14 Annual Security Report
2) ISACA's CSX Fact Sheet
3) HP`s Security begins at the endpoint WP

Кибер сигурност – Факти

- Пробив в защитата на информацията струва на компаниите средно 1,5млн за да се възстановят, с още 13% загуба на приходи. На организацията ще са нужни 9 седмици, за да се възстанови.[1]
- До 2018 г. ще има 11,4млрд свързани устройства (от 6,4млрд през 2016 г.) До 2020 г. повече от 25% от идентифицираните атаки ще бъдат свързани с интернет на нещата (IoT), със заделени по-малко от 10 % от бюджетите за сигурност.[2]

1) NTT Security Risk:Value Report 2016

2) Gartner newsroom id 3291817

Заплахата е голяма

и става все по-голяма

Кибератака – Пример

Атаката на Червея WannaCry (crypto locker ransomware) е световна кибератака, която беше насочена към компютри, работещи с Microsoft Windows, използваща уязвимост в компонента Server Message Block (SMB). Атаката започна в петък, 12 май 2017 г. и в рамките на един ден е съобщено, че са заразени повече от 230 000 компютри в над 150 държави.

Последствия – Пример

- Възстановяване на цялата система
- Преинсталиране на софтуер
- Натоварване на центъра за поддръжка
- Загуба на файлове на локалните дискове
- Неработеща периферия, напр. копир със запис на мрежови ресурс (без SMBv1)
- Несъвместимост на устройствата с по-нови версии на софтуера (напр. SMBv2)

Добри практики

за защита

ICT Media

ISACA Serving IT Governance Professionals Sofia Chapter

Добри практики – ИТ

- ✓ Операционната система на компютърните системи трябва да се поддържа актуална (Win XP не е!)
- ✓ Те работят с ефективен антивирусен инструмент, който има заредени актуализирани вирусни дефиниции.
- ✓ Използване на отделни Wi-Fi мрежи за служители и посетители, последните без достъп до локалната мрежа на организацията.
- ✓ Подсигурете, че имате контрол над крайните устройства. Създайте политики за BYOD или CYOD, като втората е за предпочитане (по-добри технологии, ергономичност).
- ✓ Включете всички устройства в обхвата, напр. услугите за печат обикновено остават сляпа зона.

Добри практики – ИТ

- ✓ Технологиите за предпазване и защита не са ефективни. Обърнете повече внимание на засичане и реакция.
- ✓ Постоянно наблюдение в реално време, използвайте крайните устройства като сензори за сигнал.
- ✓ Обучението на крайните потребители също е ключов елемент в кибер сигурността, например напомняйки на потребителя, че не трябва да кликват върху връзки или да отварят файлове в имейли, които не очакват.
- ✓ Процедурите за възстановяване при бедствия също са от ключово значение, като се гарантира, че данните се архивират редовно, така че да могат да бъдат възстановени в случай на атака.

...Комуникации

- ✓ В резултат на динамичната ситуация са възможни несъгласувани съобщения. Добре е съобщенията да се триангулират преди комуникация.
- ✓ Минимизиране на забавянето при първоначалната комуникация след установяване на инцидента.
- ✓ Актуализирани списъци с контакти, с включени номера за спешни повиквания за всички обекти.
- ✓ Едно контактно лице при такива случаи може да се окаже тясна връзка. Препоръчва се използването на екип с център за обаждания.
- ✓ Изграждане на местна браншова мрежа, в която да споделят опит, помощ и съвети по време на инцидент.

…Непрекъсваемост

- ✓ Комуникация в извънработно време с ключови лица, които не са на разположение 24x7. Това няма да бъде устойчиво за по-дълъг период от време. Трябва да се осигури подкрепа при непредвидени обстоятелства.
- ✓ Преценете дали планове за непрекъснатост на бизнеса включват адекватна устойчивост в случай на дългосрочно прекъсване на критични системи.
- ✓ Подсигурете дали всички обекти са включени в системата за известяване при инциденти или като контакти на центъра за реагиране при кризисни ситуации (напр. CERT).

Следващи Стъпки

Приемайки предположението, че друга такава атака ще се случи в някакъв момент в бъдещето:

1. Фокусът върху кибер сигурността е от първостепенно значение в работата.
2. Поуките извлечени от кибератаки да бъдат приложени за всички бизнес дейности.
3. Допълнителни стъпки за акумулиране на знания от минали инциденти.

https://cybersecurity.isaca.org/

Благодаря за вниманието!

За контакти:

Здравко Стойчев

zs@dakospace.net