Avecto - Defendpoint

BUSINESS SOLUTIONS

Proaktivna zaščita pred naprednimi grožnjami

Andrej Kreuh

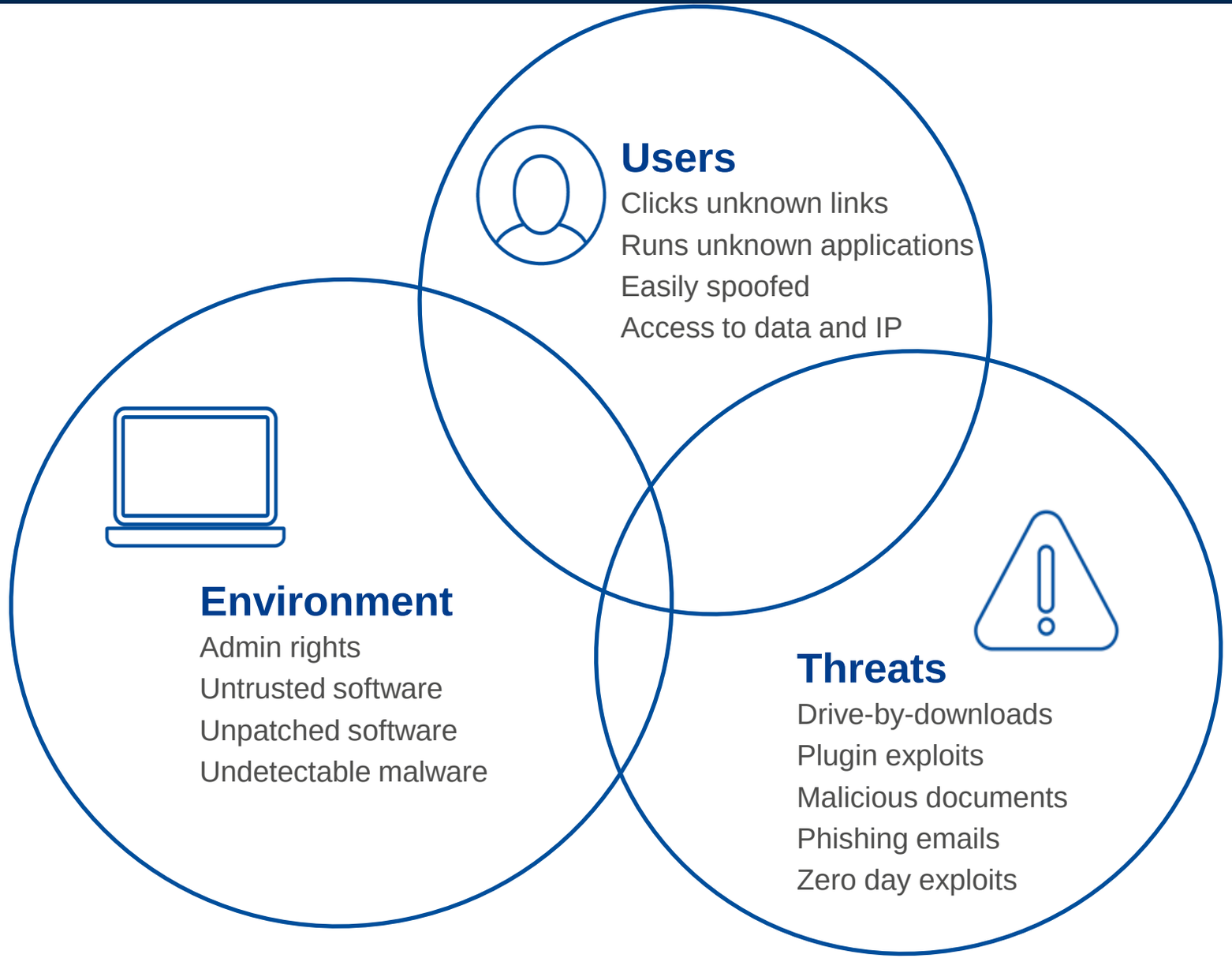
16. marec 2018

Varnostni ideali

Naprave so varne, računi **niso člani lokalne admin skupine** in nudijo **odlično zaščito pred zlonamerno kodo.**

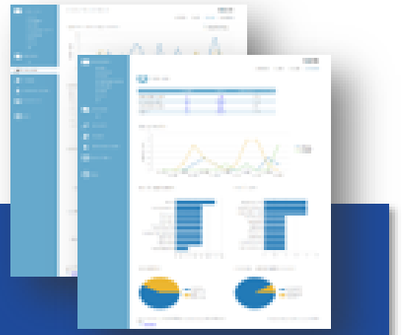
Uporabniki so produktivni, brskajo po internetu in odpirajo priponke **brez straha pred napadi**. **Sumljiva vsebina je izolirana, IT stroški pa so znižani.**

Prepreke, ki preprečujejo ideale



Trije koraki do idealnega okolja

Arhitektura



Enterprise Reporting

Centralized auditing | Reporting dashboards | Actionable intelligence

Microsoft Active Directory

Defendpoint Group Policy Edition

Policy management

McAfee

Defendpoint ePO Edition

Policy management

Client deployment

iC3 (Windows Azure)

Policy management

Built-in auditing & reporting

McAfee Security Innovation Alliance

Microsoft Partner
Gold Application Development

Primer uporabe

- Podjetje z več kot 400 strežniki
- 20 IT PRO
- 300 končnih uporabnikov
- 30 razvijalcev
- Več 10 zunanjih pogodbenih izvajalcev

9 Korakov

1. Delavnica
2. Priprava okolja
3. Pridobivanje informacij
4. Določanje načina uporabe
5. Delegacija pravic
6. Testiranje
7. Prilagajanje
8. Produkcija, odstranjevanje Admin pravic
9. Trening

Izzivi

- Razvijalci so lokalni administratorji na svojih delovnih postajah in morajo občasno ugasniti-startati sistemske servise.
- Na delovne postaje, nameščajo razvijalci komponente in programsko opremo, ki ni v sklopu internih pravil.
- Strah pred odtujevanjem podatkov, ransomware napadi in malwarom, ki ga antivirusi ne zaznajo.
- Adm_%username% računov je preveč.
- Različno izkušeni administratorji opravljajo na strežnikih različna opravila.

Izzivi

- Zunanji izvajalci vzdržujejo programe na strežnikih, vendar morajo biti v trenutku izvajanja podpore lokalni administratorji (IIS).
- Credential Guard varuje pred pass-the-hash grožnjami, vendar je še vedno veliko windows 8 delovnih postaj.
- Device Guard zahteva kriptografsko podpisane aplikacije.
- Na strežnikih in delovnih postajah ni vedno mogoče ponovno zagnati računalnika v primeru sprememb politike.
- Določene spletne aplikacije ne delujejo na Edgu, ampak potrebujejo starejše verzije IE in Chrome.

Demo

- Izsiljevalski virusi
- KeyLogger
- Portable-App
- Auditing
- Whitelisting

Na kratko…

No admin users

85% Critical Microsoft Vulnerabilities Mitigated by Removal of Admin Rights in 2015

Users are productive

“By 2018, **25%** of large organizations will have an explicit strategy to make their **corporate computing** environments **similar to a consumer computing** experience”

Gartner

IT costs reduced

“**Locked and well managed**” PCs save **$1264 per desktop**, per year. The **cost of a helpdesk ticket** for installing applications for locked-down users is **$20-$35”**

Gartner

Secure & compliant devices

Sarbanes-Oxley
Financial and Accounting Disclosure Information

Australian Government
Department of Defence

PCI DSS COMPLIANT

GCHQ

SANS

NIST

add
BUSINESS SOLUTIONS

Tbilisijska 85
1000 Ljubljana
Slovenija

info@add.si
+386 1 1 479 00 11