Kyberhyökkäyksillä ei ole valtioiden eikä instituutioiden rajoja

Petri Ramu, DNA

19.10.2016

Sairaanhoitopiirien kyberturvallisuusseminaari

Laitteiden määrä kasvaa hurjaa vauhtia

Gartner

WHY GARTNER ANALYSTS RESEARCH EVENTS CONSULTING ABOUT

Search

Newsroom

Press Release

Share: Tweet Share 1,070 G+1 +36

STAMFORD, Conn., November 10, 2015 View All Press Releases

Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015

Analysts to Explore the Value and Impact of IoT on Business at Gartner Symposium/ITxpo 2015, November 8-12 in Barcelona, Spain

Gartner, Inc. forecasts that 6.4 billion connected things will be in use worldwide in 2016, up 30 percent from 2015, and will reach 20.8 billion by 2020. In 2016, 5.5 million new things will get connected every day.

Gartner estimates that the Internet of Things (IoT) will support total services spending of $235 billion in 2016, up 22 percent from 2015. Services are dominated by the professional category (in which businesses contract with external providers in order to design, install and operate IoT systems), however connectivity services (through communications service providers) and consumer services will grow at a faster pace.

"IoT services are the real driver of value in IoT, and increasing attention is being focused on new services by end-user organisations and vendors," said Jim Tully, vice president and distinguished analyst at Gartner.

Table 1: Internet of Things Units Installed Base by Category (Millions of Units)

Category	2014	2015	2016	2020
Consumer	2,277	3,023	4,024	13,509
Business: Cross-Industry	632	815	1,092	4,408
Business: Vertical-Specific	898	1,065	1,276	2,880
Grand Total	**3,807**	**4,902**	**6,392**	**20,797**

Source: Gartner (November 2015)

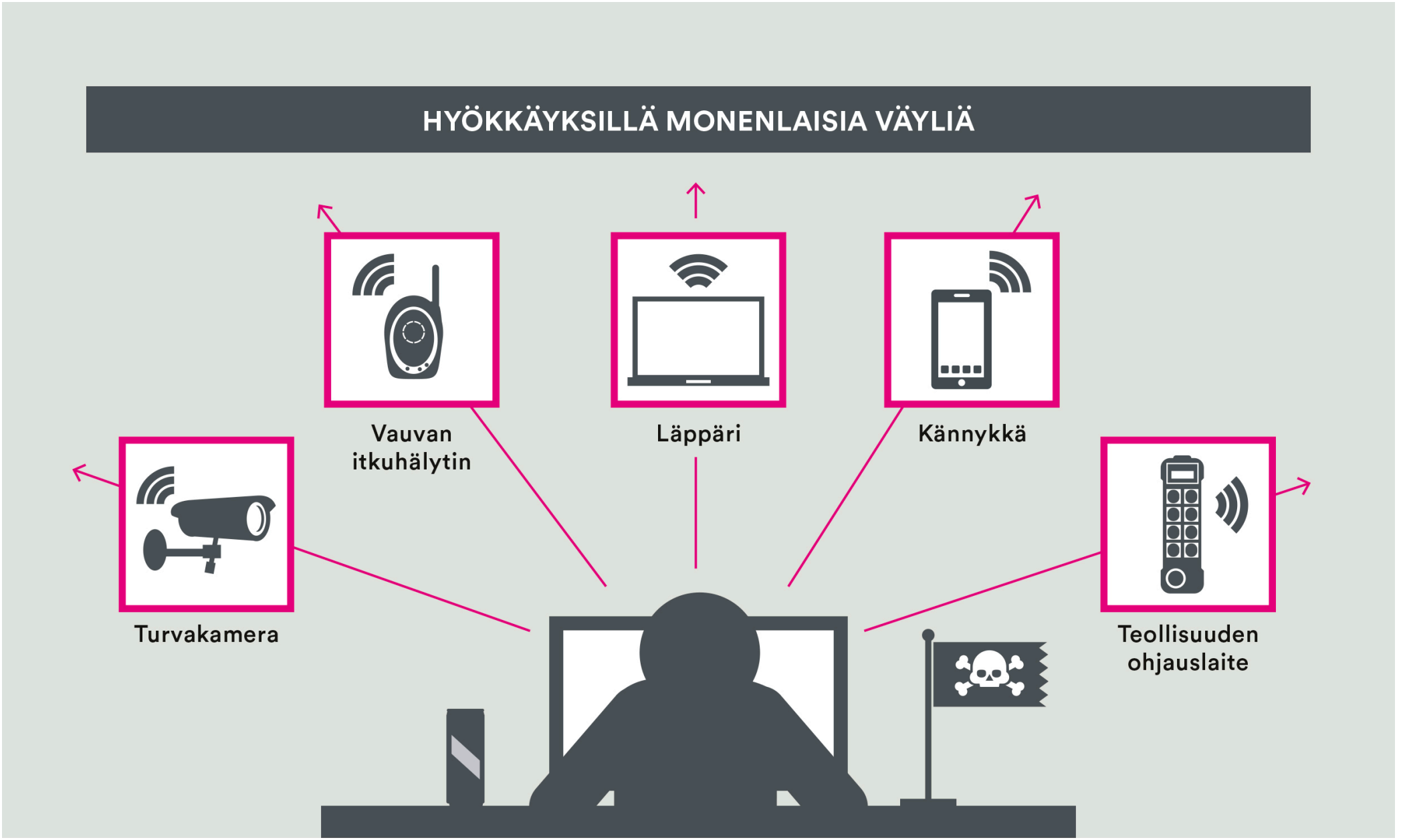
Gartnerin ennuste:

2016 → n. 6 miljardia laitetta
2020 → n. 21 miljardia laitetta

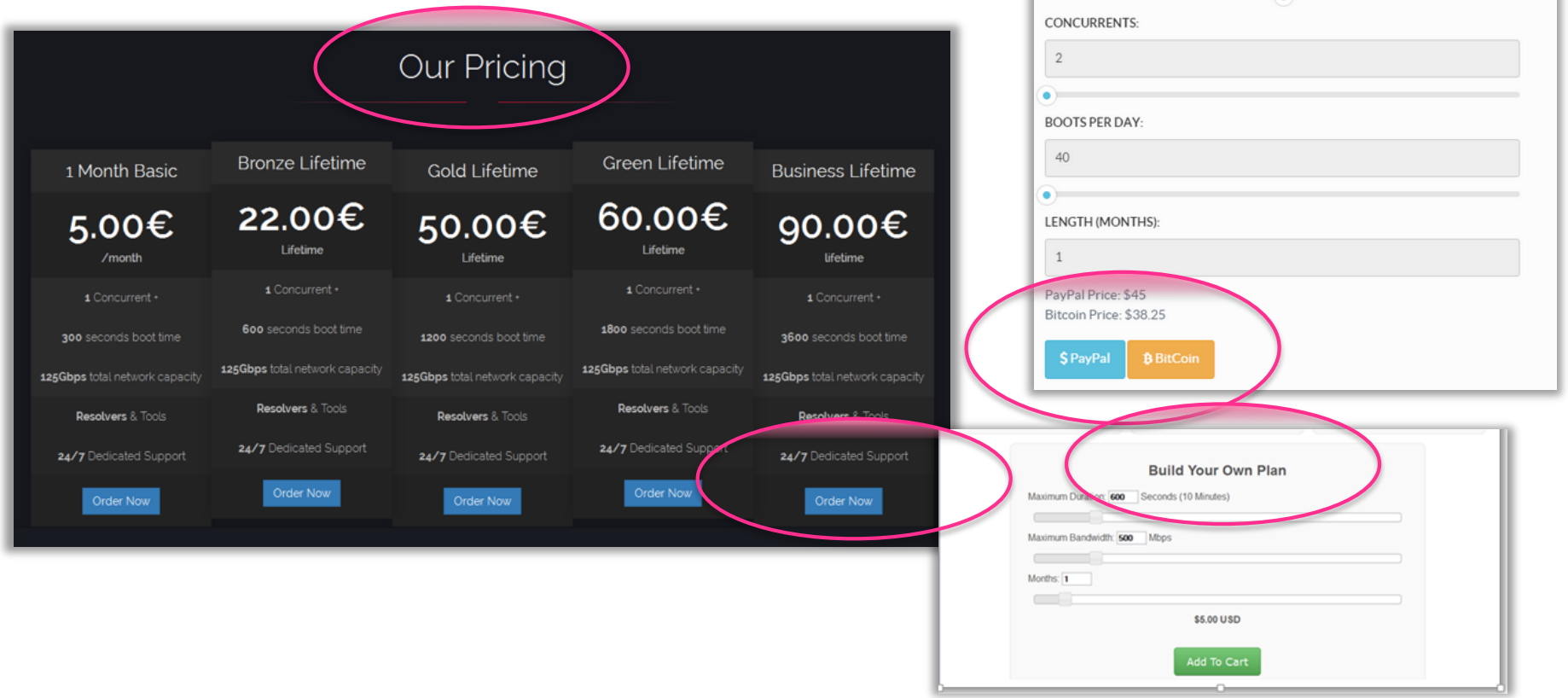
Lähde: http://www.gartner.com/newsroom/id/3165317

”IoT on kuin Internet ilman tietoturvapäivityksiä.”

Lähteet:
http://www.cio.com/article/3123492/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html#tk.drr_mlt
https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/
http://fusion.net/story/115649/hackers-breaking-into-baby-cams-are-actually-trying-to-help/
http://www.tivi.fi/Kaikki_uutiset/termostaattiin-ujutettiin-kiristysohjelma-maksa-tai-tulee-kuumat-paikat-6572281


HYÖKKÄYKSILLÄ MONENLAISIA VÄYLIÄ
Vauvan itkuhälytin
Läppäri
Kännykkä
Turvakamera
Teollisuuden ohjauslaite

Kyberrikollisuus tänä päivänä



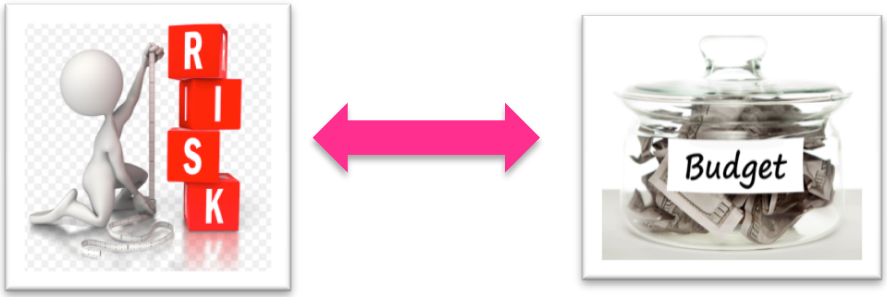
Kohdistetut hyökkäykset (Advanced Persistent Threats = APT)

- Räätälöity ja huolellisesti suunniteltu kohdistettu hyökkäys
- Kohdistuu yleensä valittuun organisaatioon tai valittuun joukkoon henkilöitä
- Hyökkäystä erittäin vaikea havaita
- Käytetyt haittaohjelmat yksilöityjä (normaalit antivirus-ohjelmistot eivät auta)
- Hyökkääjä käyttää aikaa tiedusteluun (heikon lenkin etsiminen)
- Tavallisimpia hyökkäystapoja:
  - Muistitikku
  - Sähköpostiliitteet (phishing)
  - Kiinnostavat web-sivustot
  - Sosiaalinen media
- Hyökkääjä pyrkii pysymään huomaamattomana
- Lopputuloksena tietojen siirtäminen yrityksen sisäverkosta ulos internettiin

VERKOSSA KYBERRIKOLLISTEN KAVALKADI

Miten suojautua?

- **Verkon reuna-alueen suojaaminen**
  - Next Generation Firewall and Segmentation
  - Secure Email Gateways
  - Content Filtering Proxy
  - DDoS Mitigation solutions
  - Sandboxing
  - Intrusion Detection and Prevention
  - WiFi Scanner & Air Protection
  - Link encryption Solutions
  - Strong Authentication
  - Identity Management
- **Sovellusten ja palveluiden suojaaminen**
  - Application Delivery Controllers
  - Web Application Firewall
  - Vulnerability Scanning
  - Log Management (6 month fact – Who / What/When)
  - Security Information Event Management (SIEM/SOC)
- **Laitteet**
  - EndPoint Security
  - Data Leakage Prevention
  - Device Encryption
  - Mobile Device Management

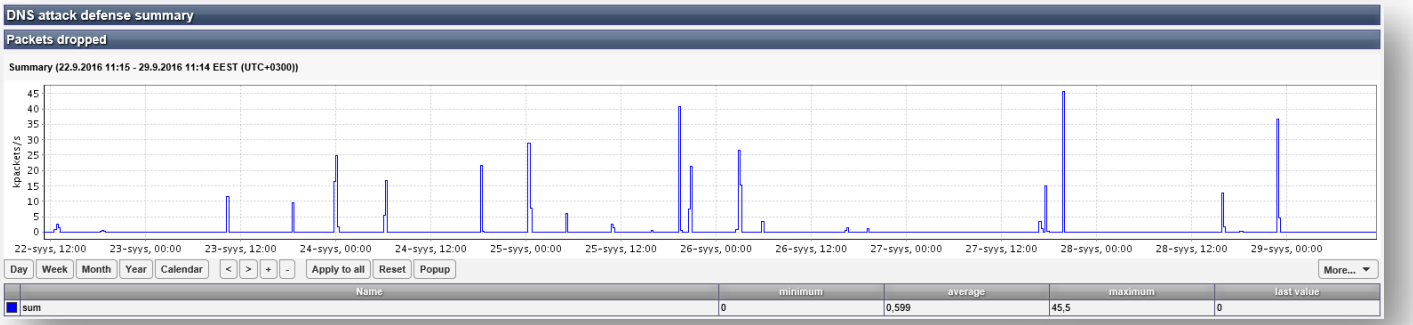


Lände: https://heimdalsecurity.com/blog/building-trust-cyber-security-guidelines-for-employees/

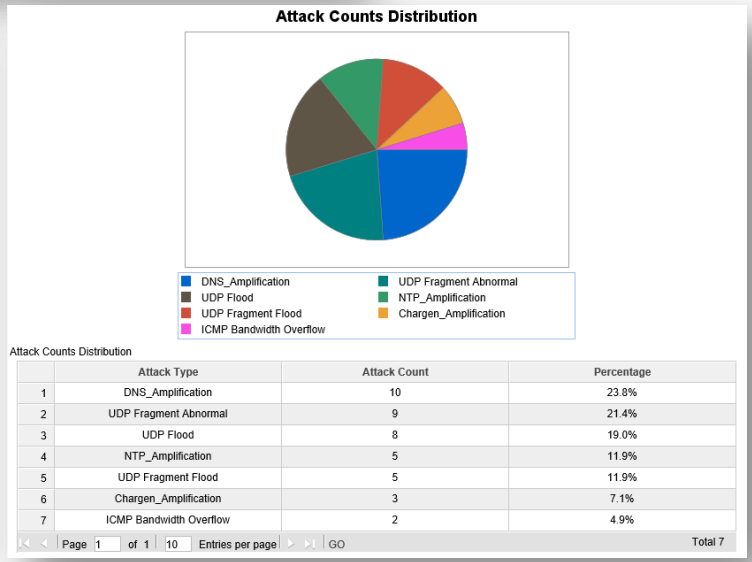
DNA:n tietoturvapalveluita maailmalla

- **DNA ylläpitää tietoturvapalveluita 55 eri maassa**
  - Tietoturvapalveluihin käytettäviä laitteistoja ulkomailla noin 700 kpl
  - Muun muassa Chile, Etelä-Korea, Intia, Kazakstan, Kiina, Panama Rep., Mexico, Qatar, Ukraina, Venäjä, USA
  - Palveluita hallitaan Helsingistä

Operaattorin rooli palveluissa



#	Date/Time	Action	Service	Destination IP	Virus	User	Threat Level
1	10:44:49	blocked		208.100.26.234	Nivdort		critical
2	10:42:51	blocked	HTTP	85.128.174.113	JS/FakejQuery.BC!tr		critical
3	10:38:42	blocked	HTTP	85.128.174.113	JS/FakejQuery.BC!tr		critical
4	10:38:42	blocked	HTTP	85.128.174.113	JS/FakejQuery.BC!tr		critical
5	10:37:15	blocked	HTTP	104.27.147.133	JS/FakejQuery.BC!tr		critical
6	10:34:02	blocked		208.100.26.234	Nivdort		critical
7	10:33:33	blocked	HTTP	85.128.174.113	JS/FakejQuery.BC!tr		critical
8	10:33:33	blocked	HTTP	85.128.174.113	JS/FakejQuery.BC!tr		critical
9	10:12:06	blocked		208.100.26.234	Nivdort		critical
10	10:03:44	blocked		208.100.26.234	Nivdort		critical
11	09:35:53	blocked	HTTP	104.192.108.21	Adware/Apptrack!Android		critical
12	09:08:11	passthrough	FTP	209.132.183.61			critical
13	08:45:25	blocked		208.100.26.234	Nivdort		critical
14	08:44:59	passthrough	HTTP	23.63.227.128			critical
15	08:44:35	blocked	HTTP	42.99.128.147	Android/Generic.S.25DC76!tr		critical
16	08:05:38	blocked		208.100.26.234	Nivdort		critical
17	07:51:52	blocked		208.100.26.234	Nivdort		critical
18	07:42:36	blocked		208.100.26.234	Nivdort		critical
19	07:31:27	blocked		208.100.26.234	Nivdort		critical
20	07:19:49	blocked		208.100.26.234	Nivdort		critical
21	07:13:26	blocked		208.100.26.234	Nivdort		critical
22	07:13:26	blocked		208.100.26.234	Nivdort		critical
23	07:04:13	blocked		208.100.26.234	Nivdort		critical
24	06:53:27	blocked		208.100.26.234	Nivdort		critical
25	06:53:27	blocked		208.100.26.234	Nivdort		critical
26	06:53:27	blocked		208.100.26.234	Nivdort		critical
27	06:38:09	blocked	HTTP	83.149.98.133	JS/FakejQuery.BC!tr		critical
28	06:29:20	blocked		208.100.26.234	Nivdort		critical
29	06:16:49	blocked		208.100.26.234	Nivdort		critical
30	06:06:26	passthrough	HTTP	93.184.215.245			critical
31	05:55:58	passthrough	HTTP	93.184.215.245			critical
32	05:55:34	blocked		208.100.26.234	Nivdort		critical
33	05:37:25	blocked		208.100.26.234	Nivdort		critical



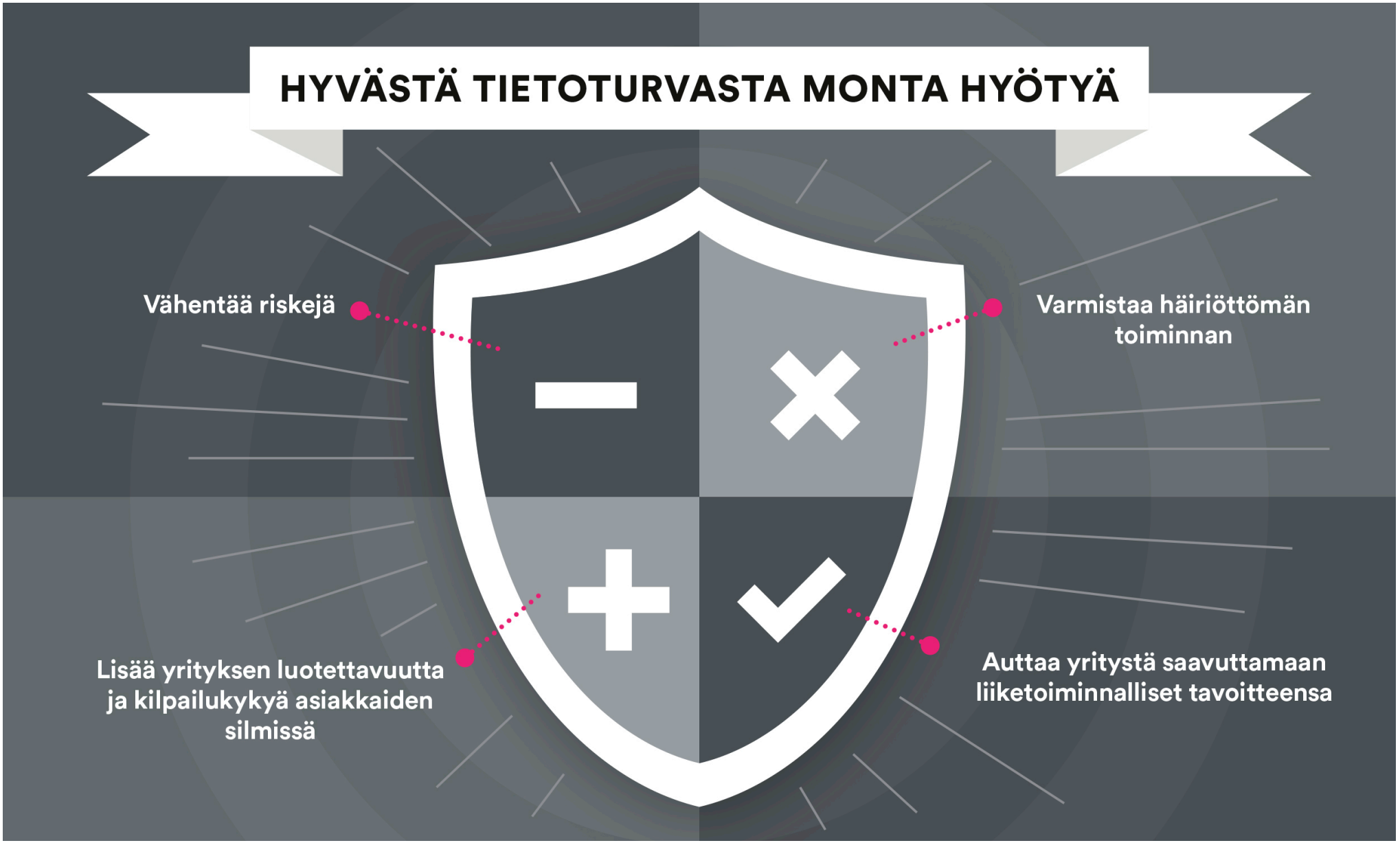
Attack Counts Distribution

	Attack Type	Attack Count	Percentage
1	DNS_Amplification	10	23.8%
2	UDP Fragment Abnormal	9	21.4%
3	UDP Flood	8	19.0%
4	NTP_Amplification	5	11.9%
5	UDP Fragment Flood	5	11.9%
6	Chargen_Amplification	3	7.1%
7	ICMP Bandwidth Overflow	2	4.9%

Page 1 of 1 | 10 Entries per page | GO | Total 7

ASKELEET PAREMPAAN TIETOTURVAAN

1. **Suunnittele** myös tietoturvaa heti digitaalisen hankkeen alkuvaiheessa.
2. **Vaadi** operaattorikumppaniltasi suunnitelma tietoturvariskien hallinnasta.
3. **Tekniset** perusratkaisut kuntoon. Muista ainakin julkisen internetin ja sisäverkon väliset tietoturvaratkaisut, sovellusten tunnistaminen, hyökkäysten estäminen ja haittaohjelmien suodattaminen.
4. **Varmista** henkilöstön kaikkien päätelaitteiden tietoturva.
5. **Luokittele** data sen kriittisyyden perusteella. Määrittele kullekin tärkeysluokalle sopiva datan säilytyspaikka.
6. **Varmista** identiteetin ja käyttöoikeuksien hallinta.
7. **Huolehdi** henkilöstön tietoturvakoulutuksesta.


HYVÄSTÄ TIETOTURVASTA MONTA HYÖTYÄ
Vähentää riskejä
Varmistaa häiriöttömän toiminnan
Lisää yrityksen luotettavuutta ja kilpailukykyä asiakkaiden silmissä
Auttaa yritystä saavuttamaan liiketoiminnalliset tavoitteensa

Kiitos!

Lisätietoja:

petri.ramu(a)dna.fi

dna.fi/yrityksille/oppaat-ja-vinkit/tietoturvaopas-kybersota-muuttuu-rajummaksi