HappyOrNot®

HappyOrNot tietoturvan ja tietosuojan toteutus

15.12.2022 Mikko Panula – DATOS teknologiafoorumi

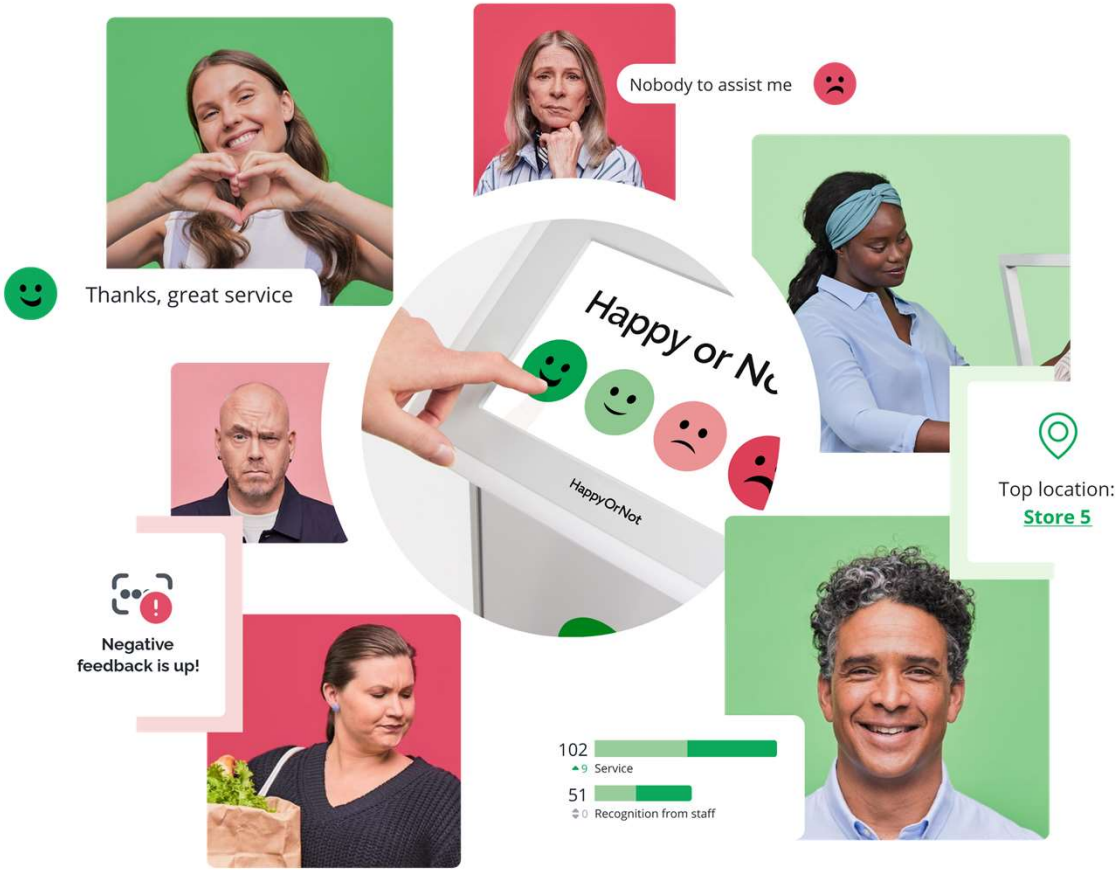
HappyOrNot®

HappyOrNot®

The pulse of meaningful feedback

The HappyOrNot solution

Convert customer feedback into more revenue



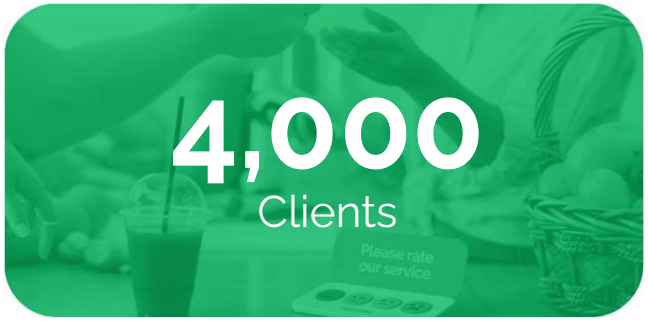
HappyOrNot®

Company highlights

Established in
2009
we are the pioneers of customer feedback

90
Employees

65
Reseller Partners



HappyOrNot

Customers worldwide

4,000 brands trust in the HappyOrNot solution for their customer experience insights

HappyOrNot®

EPO

Solution summary

Smileys

Collect lots of in-the-moment feedback from all touch points

Analytics

Understand the feedback results and act on data to improve operations

Success Services

Get expert advice, learn best practices, and improve solution use

HappyOrNot®

Slide 6

EP0 [@Stephanie Levy] I am not a fan of the green rounded boxes... What about something like this that takes the light blue format used in the "our team" slide?
Eija Paajanen; 2022-08-31T09:46:54.535

SL0 0 [@Eija Paajanen] I would not overuse the blue as it is not a "true" brand color. I recommend this.
Stephanie Levy; 2022-08-31T10:06:49.339

EP0 1 [@Stephanie Levy]Works as grey as well for me! It's more to do with the shape than the color... I think this version works fine
Eija Paajanen; 2022-08-31T10:22:29.625

SL0 2 Great! It's settled then :D
Stephanie Levy; 2022-08-31T10:25:18.290

Mikko Panula

- 44v kolmen lapsen isä Seinäjoelta
- Ohjelmistotekniikan DI TTKK 2003
- HappyOrNot, Alma Media, Universomo, Dicode, Vertex
- Internetissä vuodesta 1994
- Futis-jojo, metsästäjä, ultrajuoksija

Sisältö

1. Määritelmiä
2. Tietoturvatyö HappyOrNotilla
3. Tietosuojan alainen tieto ja suojan varmistaminen
4. Tietoturvan sipulimalli
5. Infrastruktuuri koodina
6. Monitorointi, hälytykset

HappyOrNot

Tietoturva

Vain autorisoiduilla käyttäjillä pääsy (luottamuksellisuus) virheettömään ja muuttamattomaan informaatioon (eheys) tarvittaessa (saatavuus)." (ISACA, 2008)

Informaation turvaamisen työ riskinhallinnan avulla.

Tietosuoja

- Osa perustuslain takaamaa yksityisyyden suojaa.

- Tarkoituksena on varmistaa, että organisaatiot käsittelevät **henkilötietoja** lainmukaisesti ja vain silloin, kun niiden käsittelyyn on lainmukainen peruste.

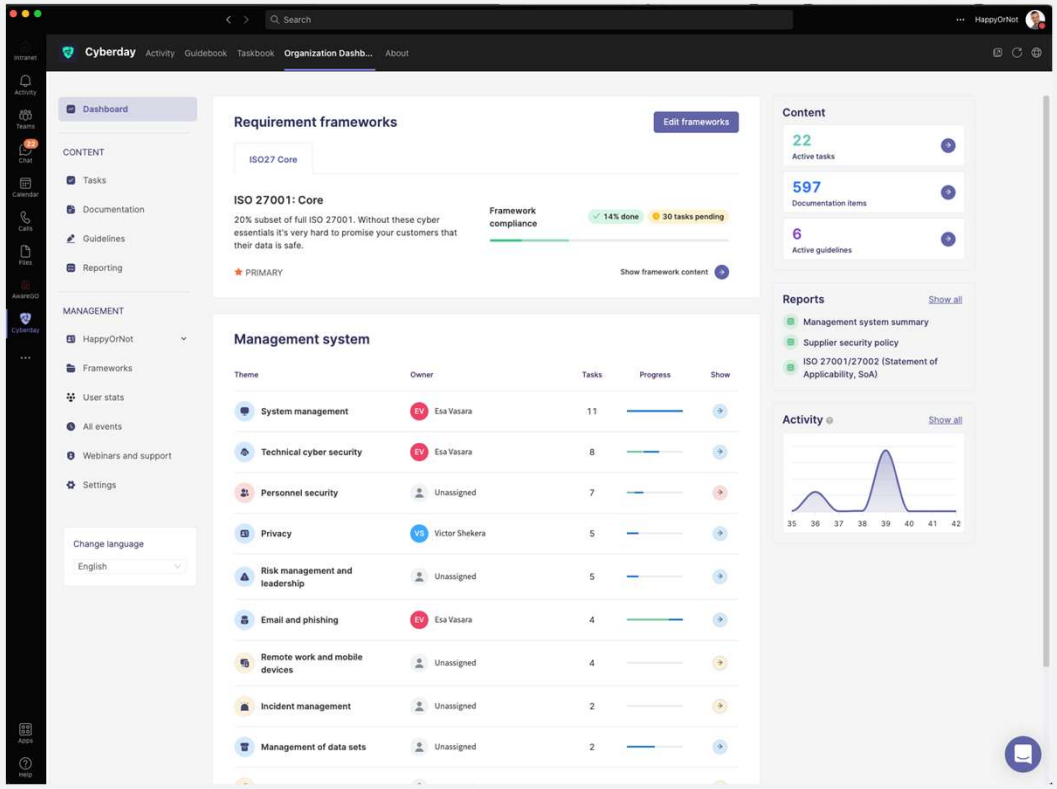
- Rekisteröidyllä on myös oikeus tarkastaa kunkin organisaation hallussa olevat henkilötietonsa ja tarvittaessa korjata niitä.

Tietoturvatyö HappyOrNotilla

- Järjestelmällinen kehittäminen vasta alkamassa
- Käytössä tietoturvan hallintatyökalu (ISMS): Digiturvamalli.fi
  - Dokumentointi käynnissä: ISO 27001 Core, GDPR
  - Tuotos:
    - Työntekijäohjeistus ja sen käytön seuranta
    - Vaatimustenmukaisuusraportit asiakkaille

HappyOrNot

Digiturvamalli.fi



HappyOrNot®

Riskienhallinta

1. Tunnista tieto-omaisuus, uhat, haavoittuvuudet ja vaikutukset
2. Arvioi riskit
3. Päätä riskeille: vältä, lievennä, jaa vastuu tai hyväksy
4. Jos päätös lieventää, toteuta/paranna tietoturvakontrolleja
5. Monitoroi / arvioi / paranna

- Lisääntynyt tietoturva vs Toteutuksen kustannukset
- Tietoturva vs Käytettävyys

HappyOrNot

HON Tietoturvan historia

- Meillä on "anonyymidata-historia"
- Asian muuttuneet vuoden sisällä
  - Palautteen jättäjän yhteystietojen keräys -ominaisuus
  - Maailmantilanne: Valtavasti tietoturvaselvityksiä asiakkailta
- Järjestelmän verkkosuojaus ollut aina hyvä
- Käytänteissä ja ohjeissa parannettavaa
- Uusimmat: AWS multi-account -ympäristö, Haavoittuvuus-skannaukset, Penetraatiotestaus, Työntekijöiden rajoitukset, Virus-skannerit jne.

Vastuunjako

- Tietoturvasta on jokainen vastuussa
- Nimetty tietosuojavastaava
- Fyysinen tietoturva: HR
- IT-palvelut:
  - Laitteiden suojaus (mobiililaitteet, läppärit,..)
  - Toimistoverkko
  - MS 365, Salesforce, Netsuite, Bezala, jne.

Vastuunjako

- HappyOrNot - Analytiikkajärjestelmä: Engineering Office

  - Järjestelmän sovellusten ja infrastruktuurin tietoturva

- Asiakkaat vastuussa omasta pääsynhallinnastaan

- Myös HappyOrNotin työntekijöillä työtehtävään perustuva pääsy asiakastietoihin

HappyOrNot

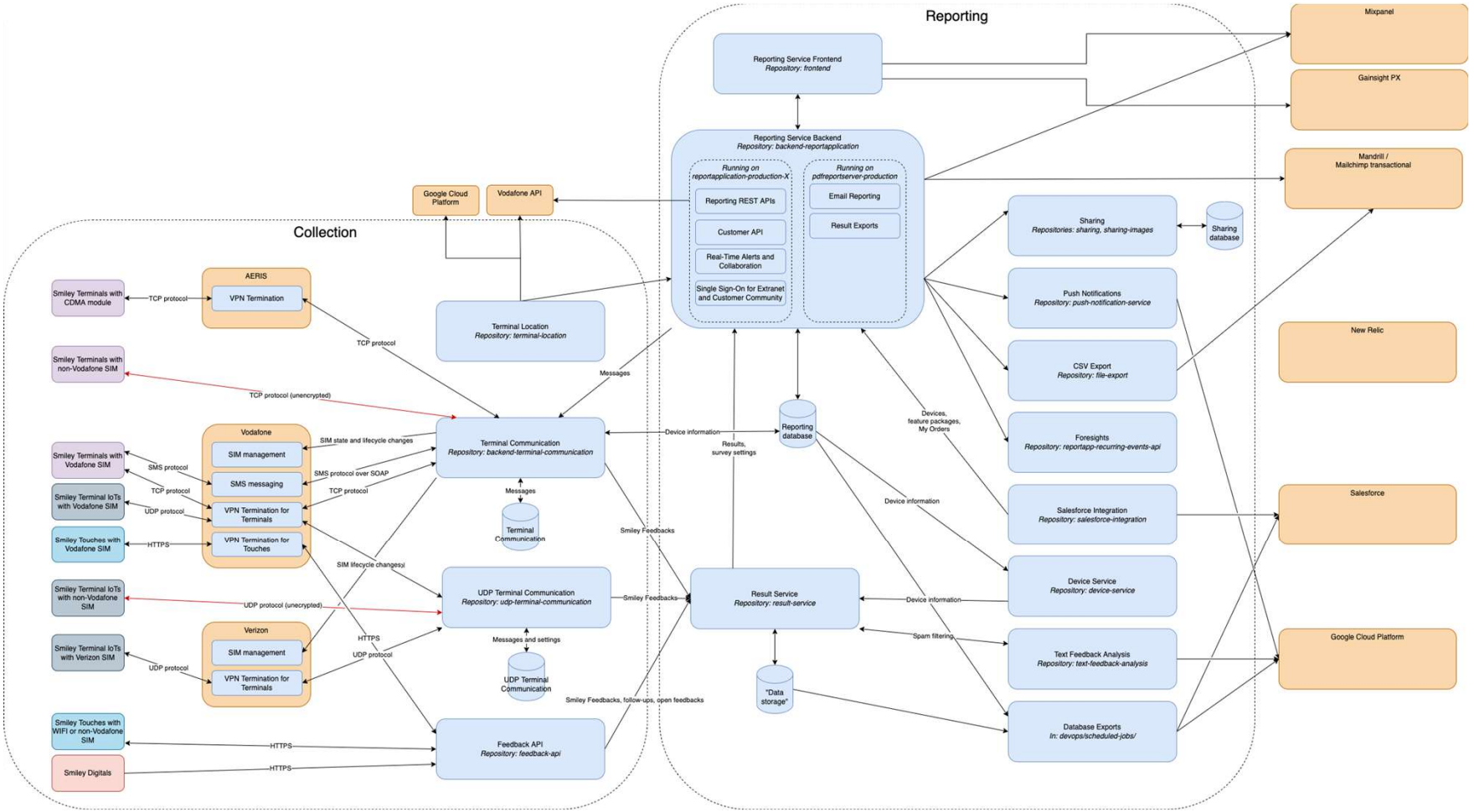
Tietosuojan alainen tieto

- Käyttäjätilit: email, etunimi, sukunimi
  - Vain tietyt HappyOrNot-työntekijät
  - Asiakkaan ylläpitäjät

- Palautteen jättäjän yhteystiedot
  - Palautteen jättäjän hyväksyttävä käsittelyehdot
  - HappyOrNot-järjestelmän ylläpito
  - Asiakkaan ylläpitäjä päättää kuka näkee
  - Tuhotaan 30pv jälkeen

HappyOrNot

HappyOrNot Analytics -järjestelmä



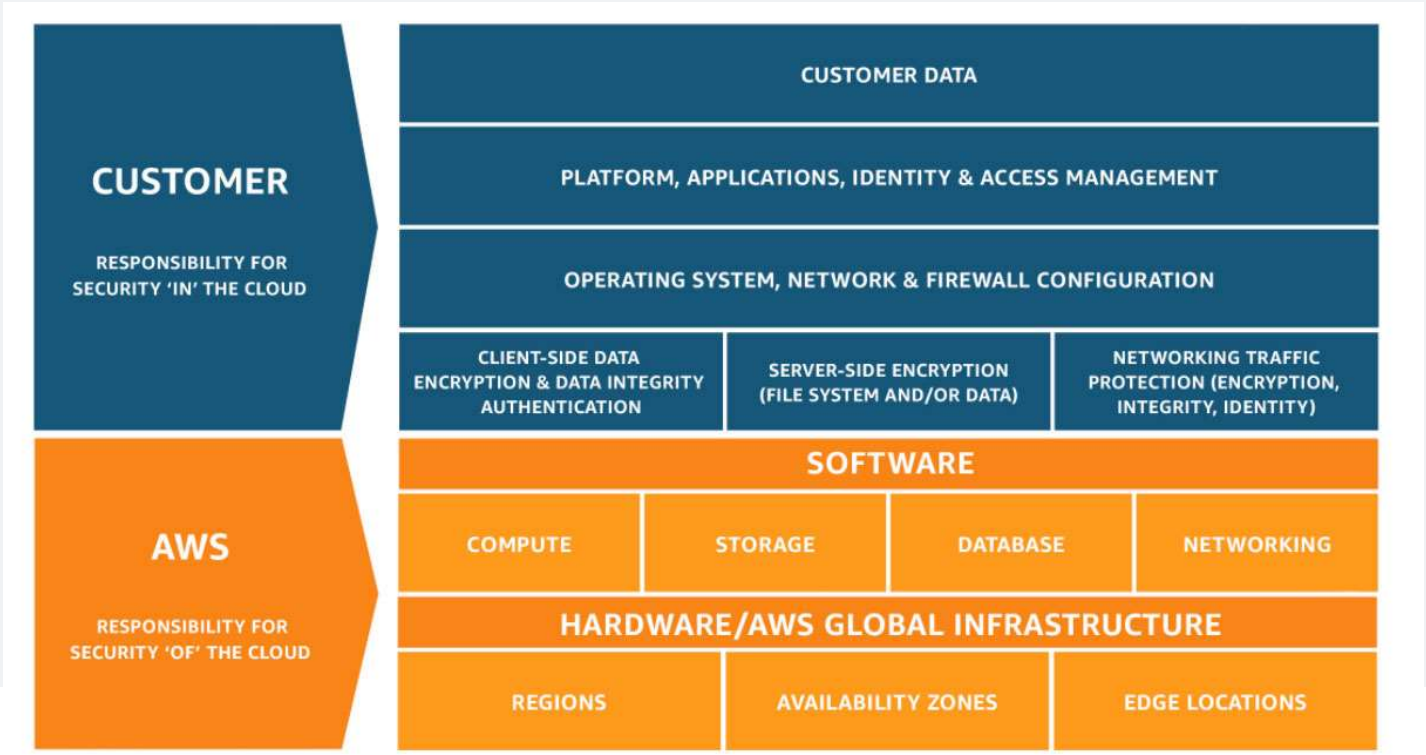
HappyOrNot Analytics -järjestelmä

- 100% AWS-pilvessä
- Useita ulkoisia yhteyksiä: Vodafone, Verizon, Aeris, Salesforce, Google APIs, Mailchimp, New Relic, Mixpanel, Gainsight
- Käyttöä 24/7, lähes kaikilta aikavyöhykkeiltä
- Yksi datakeskus (region), monta saatavuusaluetta (az)
- Teknologiat: Scala/Java, Javascript/Typescript, Postgresql
- Tukeudumme AWS:n palveluihin niin paljon kuin mahdollista
  - VPCs, EC2, Lambda, ECS, RDS, SNS/SQS, DynamoDB, ...

HappyOrNot

AWS - jaetun vastuun malli

AWS: Pilven tietoturva
HappyOrNot: Sovellusten / oman infran tietoturva



HappyOrNot

AWS:n tietoturvan toteutus

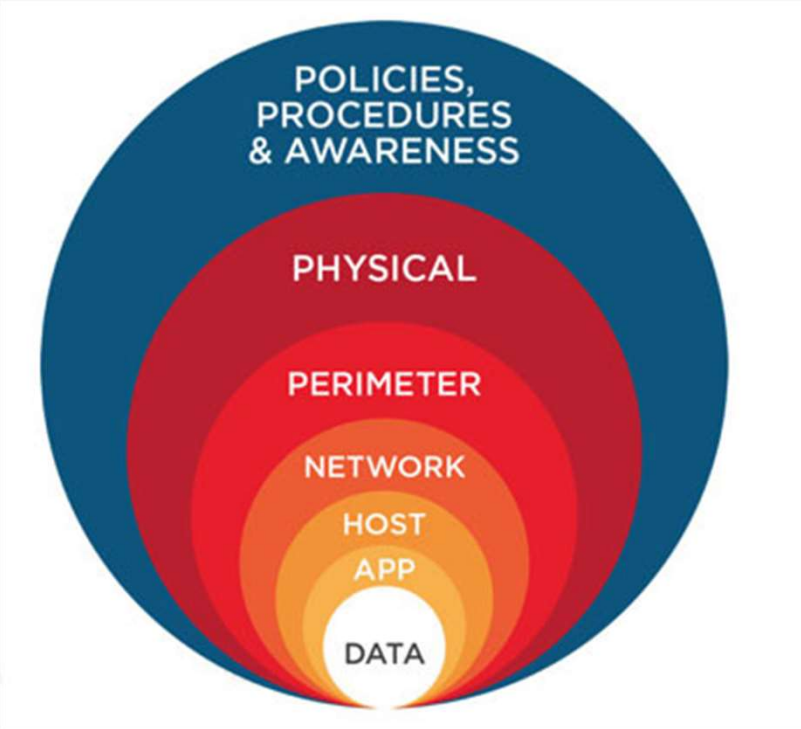
- Iso määrä käsitteitä, työkaluja, tuotteita

- Accounts, VPCs, Subnets, IGW, Route tables, NACLs, Security Groups, IAM roles,...

- Security Hub, Inspector, Detective, GuardDuty, Control Tower, Cloud Trail, Trusted Advisor, Config, Certificate Manager, Systems Manager, Key Management Service,…

- Mitä tarvitaan? Mitä maksaa?

Tietoturvan "sipulimalli" eli Defense in depth



- Käytänteet, ohjeistus, tietoturvatietoisuus
- Fyysinen tietoturva
- "Ulkokehän" tietoturva
- Sisäverkon tietoturva
- Virtuaalikoneiden/konttien tietoturva
- Sovellusten tietoturva
- Datan tietoturva

HappyOrNot

Käytänteet, ohjeistukset, tietoisuus

- Lähtökohta: luotamme omiin ihmisiimme
- Ohjeistus intranetissä kaikkien saatavilla
- Prosessit, esim. Työsuhteen alku, roolimuutos, päättyminen
- Tietoturvatietoisuus/-koulutus: AwareGO
- Päätelaitteiden käyttö
- Kehittäjien tietoturvaosaaminen

Fyysinen tietoturva

- Toimiston pääsynhallinta: Tagit, lukot
- Hälytysjärjestelmät
- Videovalvonta
- Turvallisuushenkilöstö
- Henkilöstön tietoturvatietoisuus/-osaaminen
- AWS vastaa datakeskusten osalta
- HappyOrNot: Tulli Business Park / Sponda
- Entäs kotitoimistot?

"Ulkokehän" tietoturva

- Reunareitin: AWS Internet Gateway
- Demilitarioitu vyöhyke: VPN-palvelimet
- Palomuurit: Security Groups
- Tunkeutumisen tunnistus-/estojärjestelmä (IDS/IPS): AWS Detective
- VPN:t (staging, production)
- AWS-tilitasolla erotettu sandbox / staging / production -ympäristöt

Sisäverkon tietoturva

- Automaattinen skannaus: AWS Inspector
- Verkon segmentointi: VPC, julkiset/privaatit aliverkot
- Verkon pääsylistat: NACLs, Security Groups
- Verkon liikenneanalyysi: AWS Detective

=> Tärkeimmät:

  - Security Group ingress/egress -säännöt
  - Oletus: liikenne kielletty

- Ongelma: egress-säännöt tietoturvapäivitysten asentamisessa

Virtuaalikoneiden tietoturva

- Automaattinen haavoittuvuusskannaus: AWS Inspector
- Pääsynhallinta: linux-käyttäjät/ryhmät, ssh **
  * IAM roolit, ei pääsyavaimia koneilla
- Instanssien "palomuuri": AWS Security Groups
- Porttien hallinta: AWS Security Groups
- Käyttöjärjestelmien tietoturvapäivitykset **

** = syitä pyrkiä kohti konttimaailmaa

Sovellusten tietoturva

- Palautedatan luotettavuus:
  - Painallusviive, kameran käyttö, selainsormenjälki, anomaliat
- Autentikointi:
  - Käyttäjät: email/password, SSO
  - Mikropalvelut: jaetut salaisuudet,
  - Ulkoiset palvelut: jaetut salaisuudet, Mutual TLS
- Autorisointi:
  - Käyttäjät: asiakkuus, juurikansio, käyttäjärooli
  - Muut: kovakoodattu

HappyOrNot

Sovellusten tietoturva

- Backend + frontend: syötteiden validointi
- Vuosittainen manuaalinen PenTest. Viimeisin 08/22 (Intruder.io)
- Kuukausittainen automaattinen haavoittuvuusskannaus
- Sovelluspalomuuri: AWS WAF (DoS + tunnetut haavoittuvuudet)
- Salaisuuksien hallinta: AWS Systems Manager / Parameter store

Datan tietoturva

- Salaus "lennossa": HTTPS/TSL, Operaattorien VPN:t
- Salaus "levossa": AWS Key Management Service
- Tietokantojen pääsynhallinta: tunnukset ja oikeudet
- Varmuuskopiointi toiselle AWS-tilille (Backups)
  - x krt/pv -> 1 krt/vko riippuen tietokannasta

Infrastruktuuri koodina

- Osa saatavuuden takaamista (availability)
- Tavoite: Nopea vakavistakin häiriöistä palauminen (disaster recovery)
- Työkalut: Terraform, Ansible
- Kaikki (okei, 95%) infra kuvattu määrityksillä, jotka versionhallinnassa

Monitorointi, hälytykset

- Tekninen tuki vain toimistoaikana
- New Relic, AWS Cloudwatch alarms: email + Slack
- Elintärkeä osa järjestelmää

HappyOrNot

Tietoturvatyö jatkuu..

- SSO-tuen laajennus
- ISO 27001 -työ (Digiturvamalli.fi)
- PenTest-löydösten korjaaminen
- Seuraava PenTest
- AWS Inspector, Detective -löydökset
- ...

Thank you!

HappyOrNot®