



UPPLÝSINGAÖRYGGI HVER BER ÁBYRÐ? SKÝ 2018

YFIRLIT

Hver ber ábyrgð?

Tækni

Öryggismenning

Öryggisvitund notenda



HVER BER ÁBYRGÐ?

Tækni = IT

- IT hefur hingað til borið ábyrgð á upplýsingaöryggi og þurft að kaupa sig út úr hættunum
- Auðvelt að fjárfesta á röngum stöðum með litlum ávinningi

Öryggismenning = STJÓRNENDUR

- Upplýsingaöryggi þarf að vera eins og annað öryggi, partur af stefnu og menningu fyrirtækis
- Hér bera **allir stjórnendur** ábyrgð og þurfa að leggja sitt af mörkum
- GDPR er til þess fallið að færa ábyrgðina til fyrirtækisins – nýtum það

Öryggisvitund notenda = ALLIR

- Notandinn er veikasti hlekkurinn í öryggiskeðjunni og er hann því iðulega helsta skotmark tölvuþrjóta
- Notendur þurfa að skilja tæknina betur og vita hvað ber að varast
- Hér bera **allir notendur** ábyrgð

TÆKNI — IT BUDGET

Upplýsingaöryggi verður áfram að hluta vandamál IT og það þarf budget til að kaupa nýja tækni til að leysa málin

Rannsókn IDC á 200 fyrirtækjum í Canada sýndi að:

- 23% settu minna en 6% af IT budget í upplýsingaöryggi (defeatists)
- 37% settu minna en 8% af IT budget í upplýsingaöryggi (denialists)

Alls 6 af 10 fyrirtækjum að fjárfesta undir meðaltali í upplýsingaöryggi. Þau reyndust með lágan öryggisþroska (maturity rating <3) og öryggisfrávik yfir meðaltali.

Top 40% fyrirtækin voru með öryggisfrávik undir meðaltali og hærri þroska. Þau skiptust í tvo hópa:

- Realists með 14% af IT budget og ágætis öryggi en vildu gera betur
- Egoists með 12% af IT budget voru **á toppnum** með mestan þroska (4-5) og besta árangurinn

TÆKNI — IT BUDGET

Hvers vegna var besti hópurinn ekki með mestu fjárfestinguna ?

- Meiri þroski skilar sér oft í lægri fjárfestingum með því að nota betri ferli
- Bætt innkaupaferli geta t.d. skilað lægri kostnaði með auknum kröfum til framleiðenda
- Sniðganga léleg óörugg kerfi og setja minni pening í að prófa þau og verja
- Einnig færast kostnaður út til fyrirtækisins sem hluti af öryggismenningu þess
 - Þjálfun
 - Æfingar
 - Forvarnir

Við kaupum okkur ekki út úr vandanum með tólum einum saman

https://www.theregister.co.uk/2015/08/18/responsibility_for_it_security/

TÆKNI — EINFALDAR LAUSNIR

Einfalda lausnir eins og hægt er til að berjast á sem fæstum vígstöðvum

- Ef það er allt í drasli, olía, gas og tuskur í bílskúrnum.... ekki kaupa bara annan reykskynjara

Hafa grunnþjónustur í lagi með góðu skipulagi

- Uppfærslur þurfa að vera í topp standi
- Vírusvarnir og spam varnir í gangi
- Umgengni, lykilorðapolicyur og 2FA
- Skilríkjavæðing á búnaði (enrollment)

Þá skiptir máli að spyrja rétta aðila góðra spurninga:

- Hvað gerist ef við gerum þetta ekki?
- Getum við leyst þetta á annan hátt?
- Getum við breytt vinnulagi eða arkitektúr?
- Getum við fært eða einfaldað varnarlínuna?

ÖRYGGISMENNING

Hver er öryggismenning fyrirtækisins?

Er öryggisstjóri? Er upplýsingaöryggisstjóri?

Er verið að nota „secure coding“ í þróun? (t.d. OWASP)

Er regluleg kennsla fyrir alla í upplýsingaöryggi?

Eru reglulegar æfingar eða veikleikaprófanir?

Er til samskiptaáætlun og viðbragðsáætlun?

Er verið að fylgja ISO27001?

Getum lært mikið af því hversu vel hefur tekist í framþróun á raunlægu öryggi á vinnustöðum seinustu ár.

Það er ekki lengur púkó að vera öruggur



ÖRYGGISMENNING

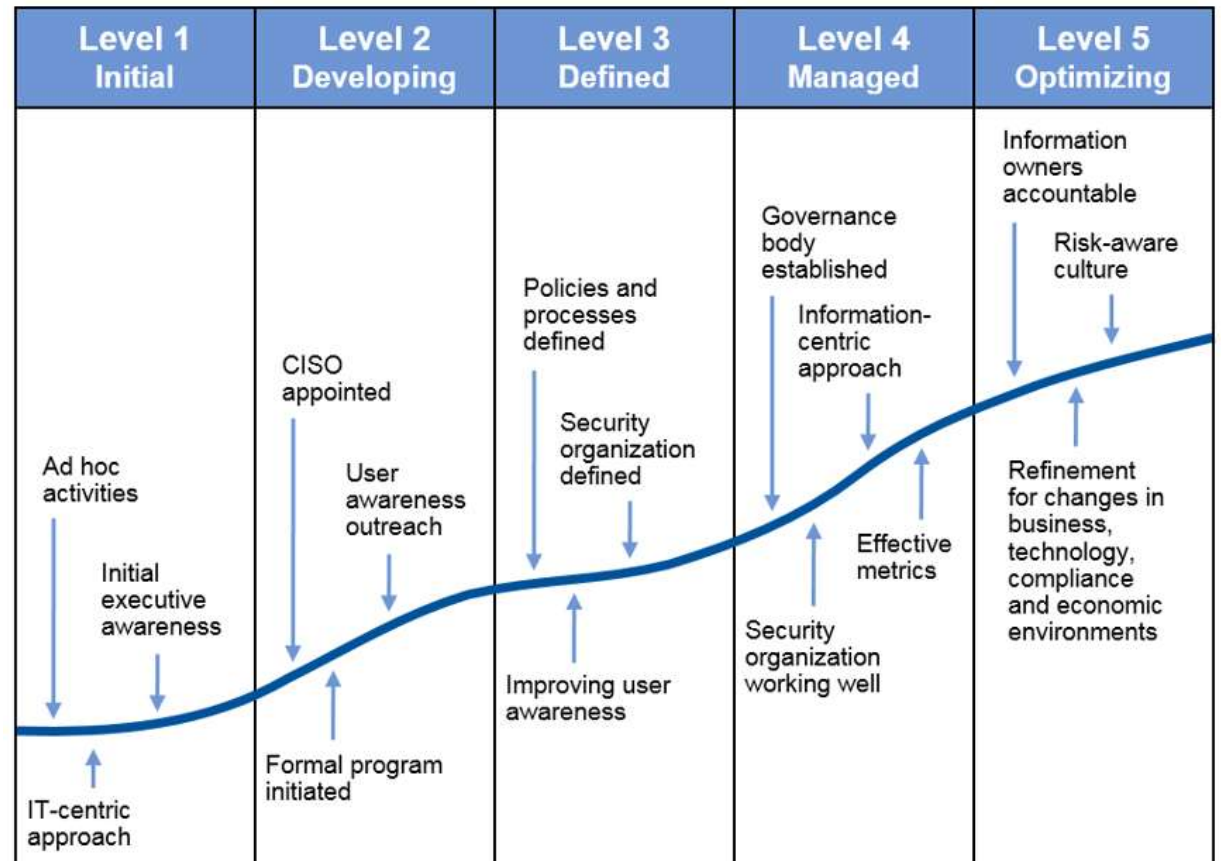
Gartner „ITScore for Information Security“

Eitt tólið sem hægt er að nota til að skilgreina öryggisþroska og ferðalagið

Þetta er fyrst og fremst sameiginlegt ábyrgðarhlutverk stjórnenda fyrirtækis

IT þarf að aðstoða við þessa þróun, ekki bara gera Level 1 dýrara

GDPR hjálpar fyrirtækjum hér ef því er tekið fagnandi og látið keyra framþróun



Source: Gartner (February 2016)

ÖRYGGISVITUND NOTENDA

Upplýsa alla stjórnendur um grunnþætti upplýsingaöryggis

- Hlutverkin, öryggisráð, ferlin sem þarf ofl.
- Taka út frá GDPR og maturity módelum

Kynna almennt upplýsingaöryggi fyrir öllum starfsmönnum og viðhalda stöðugum áróðri

Hverjar eru hætturnar í umhverfinu?

- Þjófnaður
- Hacking
- Phishing / spear phishing
- Malware
- Gögn á glámbekk

Kenna notendum að sjá hætturnar og hvernig þeir geta varist þeim?

SAMANTEKT

Öryggismenning:

- Keyra af stað með stjórnendum og tryggja fullan stuðning
- Nota GDPR sem drifkraft

Öryggisvitund:

- Byggja upp nauðsynlega þekkingu
- Festa regluverk í sessi með stöðugum umbótum og markaðssetningu
- Taka upp mælingar

Tækni:

- Fylgja eftir með réttum tólum og tækjum
- Leita að einföldun lausna og henda gömlum lausnum

ÞÚ BERÐ ÁBYRGÐ!



cyber
security

Shift

YFIRLIT

Öryggi gagna

Físískt aðgengi

Stýrikerfi

Net og internet

Phishing

Malware

5 einfaldar reglur

ÖRYGGI GAGNA

Megin leiðir að gögnum:

- Fá veltta í hendurnar
- Setur nið fylkingar
- Stæling and tæking

Meira veltta á neti og nýja velttala:

- Neting
- Setja upp Malware - Överser

Fá notendurn til að afhenda þou á Internetinu:

- Phishing
- Setja upp Malware - Överser
- Líta notanda netja spólu



FÍSÍSKT AÐGENGI

Útgangni

- Tryggja aðgangni nið
- Leta nið
- Ekki láta stölu veltta á tæknitæki
- Ekki gefa frá sér lykilar

Tæknitægi varnt:

- Dulskjala data
- Stæring stýrikerfa
- Lyklaröngur



STÝRIKERFI

Útgangni

- Setja ekki upp fylkingar á vélum
- Stöðva ekki á vörum
- Frættu ekki upphættum

Tæknitægi varnt:

- Regluleg upphættir stýrikerfa og fylkinga
- Viltur vírusvarnt
- Viltur endurbætur




NET OG INTERNET

Útgangni

- Hið er PHISHING
- Stælla ekki á bál tæki
- Ótta að fara upp lykilar og pass af malvar er það er það
- Setja ekki upp velttana fylkingar
- Frættu ekki á notendur af þou
- Leta ekki veltta

Tæknitægi

- Reyna að tryggja nið varntækt með tæki
- Núna VPN nið að setja nið og varntækt



PHISHING

Sé viltanlega stætt nið að senda dæltu tölvapósta undir merkingu viltanlega fyrirtækja í þeim tilgangi að fá eintaklingu nið að gefa upp persónulegar upplýsingar á borð við lykilar og kreditkartaupplýsingar

Þessir póstar senda saman af þou á viltu sem líta aðvæntlega eins út og viltu fyrirtækis



MALWARE

Ýmis óvartu sers óviltu er að skemma eða stölu upplýsingar

- Nýja sér velttala í stýrikerfi/kerfi nið að skemma nið
- Nýja sér viltu notanda nið að skemma nið

Leggandi - óvartu

- Viltur/tæknitægi
- Stæring/óviltu tæki
- Tægi kerfi
- Ekki getur nið viltu viltu tæki kerfi nið að skemma nið
- Ekki getur viltu tæki kerfi nið að skemma nið



5 EINFALDAR REGLUR

- Ekki smella á tæki í óvartum tölvapósti
- Aftagðu hvert stölu á tæki viltu
- Ekki opna viltu tæki úr óvartum tölvapósti
- Uppfærðu fylkingar á tæki
- Notaðu miltvarntækt lykilar á tæki

ÖRYGGI GAGNA

Megin leiðir að gögnunum

Fá vélina í hendurnar

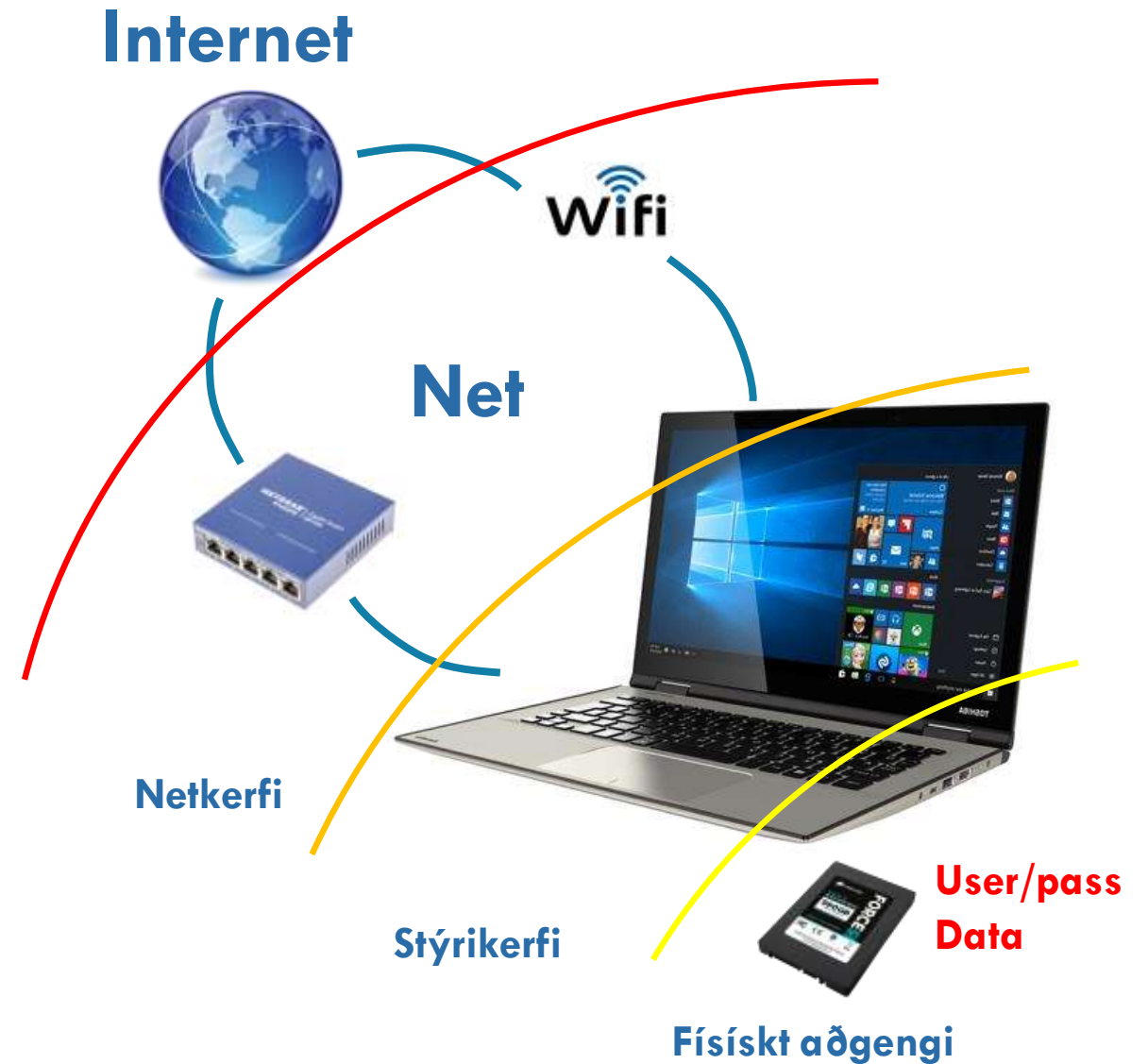
- Setjast við lyklaborðið
- Stealing and hacking

Hlera vélina á neti og nýta veikleika

- Hacking
- Setja upp Malware - Óvætur

Fá notandann til að afhenda þau á Internetinu

- **Phishing**
- Setja upp Malware – Óvætur
- Láta notanda sækja sjálfur



FÍSÍSKT AÐGENGI

Umgengni

- Tryggja aðgang að vél
- Læsa vél
- Ekki láta stela vélinni á ferðalögum
- Ekki gefa frá sér lykilorð

Tæknilegar varnir

- Dulkóða diska
- Læsing stýrikerfis
- Lykilorðareglur

Internet



Wifi

Net



User/pass
Data

Físískt aðgengi

STÝRIKERFI

Umgengni

- Setja ekki upp hugbúnað á vélinni
- Slökkva ekki á vörnum
- Fresta ekki uppfærslum

Tæknilegar varnir

- Regluleg uppfærsla stýrikerfis og hugbúnaðar
- Virkar vírusvarnir
- Virkar innbrotavarnir

Internet



Wifi

Net



Stýrikerfi



Físíkt aðgengi

User/pass
Data

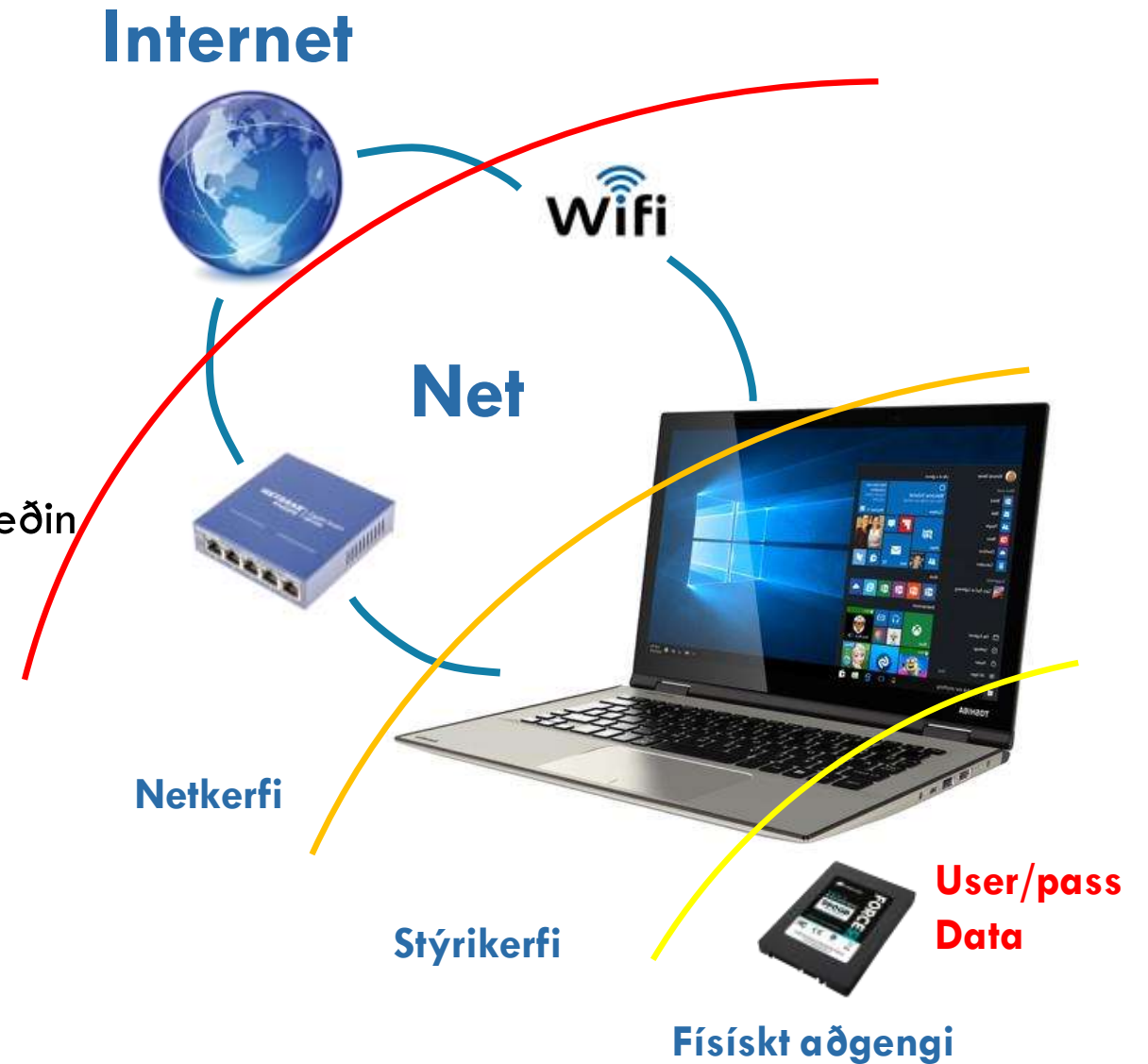
NET OG INTERNET

Umgengni

- Hvað er PHISHING?
- Smella ekki á bull linka
- Gefa aldrei upp lykilorð og pass ef maður er beðin um það
- Setja ekki upp vafasaman hugbúnað
- Fara ekki á vafasamar síður
- Lána ekki vélina

Tæknilegt

- Reyna að tryggja öll samskipti með https
- Nota VPN til að verja vél og samskipti



PHISHING

Sú sviksamlega starfsemi að senda dulbúna tölvupósta undir merkjum virðulegra fyrirtækja í þeim tilgangi að fá einstaklinga til að gefa upp persónulegar upplýsingar á borð við lykilorð og kreditkortaupplýsingar

Þessir póstar senda mann oft inn á síður sem líta nákvæmlega eins út og vefsíður fyrirtækisins



ÞEKKJA PHISHING PÓSTA OG SÍÐUR



The image shows a browser window displaying a phishing website. The address bar contains the URL <http://www.frfacebok.com>, which is highlighted with a red box and a green arrow pointing to it. The page header features the Facebook logo on the left and a login form on the right with fields for 'Email' and 'Password', and a 'Log In' button. Below the header, the text 'This is NOT FACEBOOK' is written in large yellow letters, followed by 'This is a Phishing SCAM' in red. To the right of this text is 'EXAMPLE #4'. The main content area includes a sign-up form with fields for 'First Name', 'Last Name', 'Your Email', 'Re-enter Email', and 'New Password', along with dropdown menus for 'I am: Select Sex:', 'Birthday: Month:', 'Day:', and 'Year:'. A green 'Sign Up' button is at the bottom of the form. On the left side, there is a world map with orange person icons connected by dashed lines, and the text 'Facebook helps you connect and share with the people in your life.' Below the map, it says 'Only Log into Facebook @ WWW.FACEBOOK.COM'. The footer contains language options (English (US), Español, Português (Brasil), Français (France), Deutsch, Italiano, العربية, हिन्दी, 中文(简体), 日本語, ...) and navigation links (Facebook © 2011 - English (US), Mobile, Find Friends, Badges, People, Pages, About, Advertising, Create a Page, Developers, Careers, Privacy, Terms, Help).

5 EINFALDAR REGLUR

Ekki smella á hlekk í óvæntum tölvupoósti

Athugaðu hvert slóðin á hlekk vísar

Ekki opna viðhengi úr óvæntum tölvuósti

Uppfærðu hugbúnað á tölvum

Notaðu mismunandi lykilorð á miðlum

ÞÚ SKIPTIR ÖLLU MÁLI!

