TÖLVU- OG UPPLÝSINGAÖRYGGI ÁSAMT ÖRYGGI TÆKJA IOT

Morgunverðarfundur FIE

25. maí 2016

Svavar Ingi Hermannsson
CISSP, CISA, CISM

YFIRLIT

- Hver er ég?
- Þróun í tölvu- og upplýsingaöryggi.
- Helstu hætturnar á Íslandi.
- Mikilvægi tölvuendurskoðunar.
- Hvað getum við gert betur?

HVER ER ÉG?

Svavar hefur sérhæft sig í hugbúnaðarþróun og upplýsingaöryggi undanfarin 20 ár og hefur gengt ýmsum störfum tengt hugbúnaðarþróun og tölvuöryggisráðgjöf. Svavar er með mikla reynslu í innbrotsprófunum, veikleikagreiningum, kóðarýni með tilliti til upplýsingaöryggis, innleiðingu stjórnkerfa upplýsingaöryggis m.a. ISO/IEC 27001, PCI-DSS og PA-DSS.

Svavar hefur kennt tölvuöryggi við Háskólann í Reykjavík og Háskóla Íslands.

Svavar var formaður faghóps um öryggismál hjá Skýrslutæknifélaginu 2007 – 2012.

Svavar hefur haldið fjölda fyrirlestra á Íslandi, Þýskalandi, Bretlandi, Bandaríkjunum og Úkraínu, meðal annars á Hacker Halted Europe, BSides, OWASP og UISGCon.

Svavar er með ýmsar gráður teng upplýsingaöryggi, meðal annars: CISSP, CISA og CISM

ÞRÓUN UPPLÝSINGAÖRYGGISMÁLA

Hverjar eru helstu áhætturnar?

ÞRÓUN Í TÖLVU- OG UPPLÝSINGAÖRYGGI

- Verizon Data Breach Investigation Report 2016
  - 100.000 incidents.
  - 3.141 Data Breaches.
    - 89% of breaches had a financial or espionage motive.
  - 80% from external actors.
- Fjöldi öryggisveikleika opnaðir / tilkynntir á dag > fjöldi lokaðra / lagaðra.
- 10 – 100 days from vulnerability disclosure until exploited.

ÞRÓUN Í TÖLVU- OG UPPLÝSINGAÖRYGGI

- Phishing árásir
  - 8.000.000+
    - 30% opnuðu tölvupóst
    - 12% opnuðu hlekk / viðhengi
- Dark Reading (http://www.darkreading.com/)
  - Healthcare Suffers Estimated $6.2 Billion In Data Breaches
  - Nearly 90 percent of healthcare organizations were slammed by a breach in the past two years.

ÞRÓUN Í TÖLVU- OG UPPLÝSINGAÖRYGGI

- Office of Personnel Management data breach (8 million government employees), including detailed security-clearance-related background information. – Product demonstration.

- An $80M Bank Hack Has Been Blamed on $10 Routers – Bangladesh bank
  - $850-$870 million transfer stopped due to typo.

HELSTU HÆTTURNAR Á ÍSLANDI

Skortur á þekkingu á sviði upplýsinga-öryggis

MESTA ÁHÆTTAN – SKORTUR Á ÞEKKINGU

6 / 4

15 / 7+?

16 / 20?

4 / 8?

MESTA ÁHÆTTAN – SKORTUR Á ÞEKKINGU

Öryggisstjóri
7 (12)

CISO
6 (12)

CSO
7 (24)

Forstjóri
|
Fjármálastjóri
|
Yfirmaður Tölvudeildar
|
Öryggisstjóri

ÁHÆTTUR

"117 million LinkedIn passwords sold by hackers" – The Register

ÁHÆTTUR

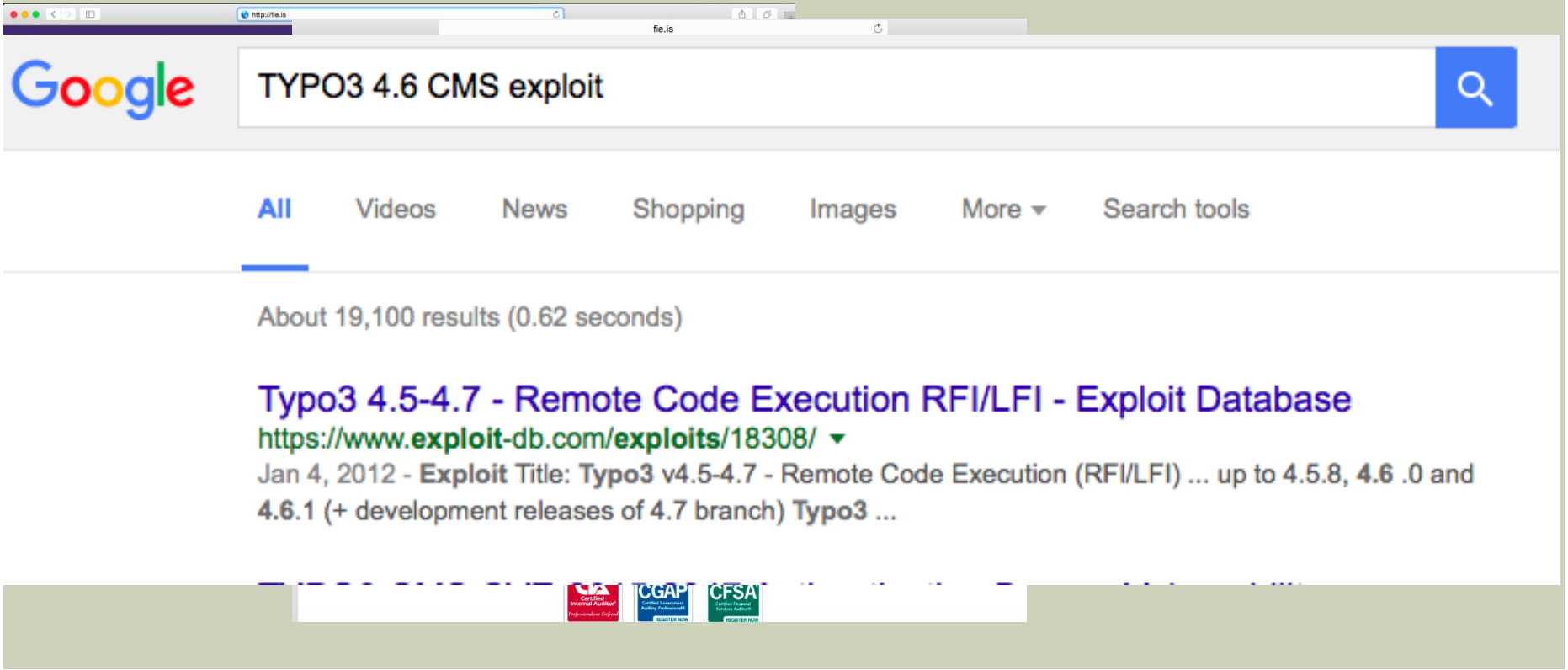
Gagnagíslataka

Fjárkúganir

Almennt svindl

HVAÐ ER ÖRYGGISVEIKLEIKI?

ÁHÆTTUR – HTTP://FIE.IS



ÁHÆTTUR - PANAMA

ÁHÆTTUR - FJÁRMÁLAKERFI + VEFFORRITUN

Microsoft Dynamics™ NAV

+

MIKILVÆGI TÖLVUENDURSKOÐUNAR

Hvað getum við gert betur?

HVAÐ GETUM VIÐ GERT BETUR?

- Kröfur til okkar?
- Krafa á hýsingaraðila?
- Krafa á rekstraraðila?
- Krafa á hugbúnaðarhús?

KRÖFUR TIL OKKAR - ALMENNT

- Stjórnun aðgangs
- Breytingastjórnun
- Öryggisafritunartaka og endurheimt gagna
- Áhættumat / áhættumeðferðaráætlun
- Áætlun um samfelldan rekstur
- Frávikaskráning
- Raunlægt öryggi (e. physical security)
- Innra eftirlit

HVAÐ GETUM VIÐ GERT BETUR? – VIÐBÓTARKRÖFUR

- Krafa um öryggisuppfærslur.
- Vöktun á öryggisuppfærslum.
- Hvað er öryggisúttekt?
  - Mismunandi tegundir.
- Er úttektin framkvæmd af óháðum þriðja aðila?
- Er úttektin skjalfest?
- Er hægt að fá afrit af öryggisúttektarskýrslunni?
- Fara fram á öryggisuppfærslur.

HVAÐ GETUM VIÐ GERT BETUR? - TÖLVUINNBROT

- Tölvuinnbrot – Hverjum ber að tilkynna?

HVAÐ GETUM VIÐ GERT BETUR? – KAUP Á HUGBÚNAÐI

- Er viðkomandi með ISO/IEC 27001 vottun?
- Er verið að fylgja alþjóðlegum stöðlum um örugga hugbúnaðarþróun?
- Hafa verið framkvæmdar öryggisúttektir?
- Tilkynning öryggisveikleika?
- Öryggisuppfærslur?
- Öryggisstjóri?

HVAÐ GETUM VIÐ GERT BETUR? - ÞJÓNUSTUAÐILAR

- Er viðkomandi með ISO/IEC 27001 vottun?
- Um stjórnun aðgangs?
- Um öryggisafritunartöku?
- Um breytingastjórnun?
- Um öryggisuppfærslur?
- Um rekstrar / upplýsingaöryggisfrávik?
- Um öryggisstjóra?
- Um öryggisúttektir?

HVAÐ GETUM VIÐ GERT BETUR? - HÝSINGARAÐILAR

- Er viðkomandi með ISO/IEC 27001 vottun?
- Áætlun um samfelldan rekstur?
- Breytingastjórnun?
- Öryggisafritunartaka?
- Um rekstrar / upplýsingaöryggis frávik?
- Um öryggisuppfærslur?
- Öryggisúttektir?
- Öryggisstjóri?

TAKK FYRIR

SVAVAR@SECURITY.IS

Morgunverðarfundur FIE

25. maí 2016

Svavar Ingi Hermannsson
CISSP, CISA, CISM