NEXON

IT-KIKÖTŐ 2017

GDPR – Adatvédelem újratöltve

kihelyezett

hub club

A GDPR ICT-vonatkozásai

Csizmazia Darab István
Sicontact, IT biztonsági szakértő

Tartalom

:: GDPR - Ezmiez?

:: Változások, kihívások

:: Tanulópénzek

:: A szakma lehetséges feladatai

:: Biztonság+tudatosság

IT-KIKÖTŐ 2017 GDPR-Adatvédelem újratöltve

GDPR - Ezmiez?

- 2018. május 25.
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- Kidolgozott és érvényes, elfogadott uniós jogszabályok gyűjteménye
- Meghatározzák az ország forrásainak, adatainak védelmét
- Elősegítik az állami, illetve a magánszektor közötti együttműködést
- Jogokat biztosít az uniós állampolgároknak adataik kezelésével kapcsolatban

IT-KIKÖTŐ 2017 GDPR-Adatvédelem újratöltve

GDPR - Ezmiez?

Személyes adat: minden olyan információ, ami egy azonosított vagy azonosítható természetes személyre vonatkozik

- Minden EU területén tevékenykedő cég
- Minden uniós polgárok adatait kezelő szervezet (nem csak az EU-ban működő)
- Legfőbb szegmens a szenzitív adatok kezelők: EÜ, oktatás, kormányzat
- A szabályozási rendszer igen összetett, fokozott adatbiztonsági követelmények
- Erősebb hatósági felügyelet, magasabb (20 mEUR) bírság

IT-KIKÖTŐ 2017 GDPR-Adatvédelem újratöltve

Változások, kihívások

Milyen változásokat hoz mindez?

A "kockázatarányos védelem elve"
- Például az egészségügyi szektorban

Megfordul a bizonyítási teher
- Fontos új alapelv: az elszámoltathatóság elve
- Nem elég, ha az adatkezelő betartja az adatvédelmi szabályokat, igazolnia is kell a megfelelést

Változások, kihívások

Értesítési kötelezettség

- adatvédelmi incidensek esetére előírt értesítési kötelezettség

- jelentős többletterhet ró az adatkezelő szervezetekre

- az incidensek ügyfelek felé történő kommunikációja rombolhatja az ügyfelek szervezet iránti bizalmát, ronthatja a szervezet jó hírét

- halogatása, elhallgatása, kozmetikázása viszont tönkreteheti a céget

- Módosítási javaslat: mentesség, ha a szervezet alkalmazta a technikai és szervezési védelmi intézkedéseket, például titkosítás

Változások, kihívások

Az érintettek számára meghatározott jogok biztosítása

- Mind a hatályos hazai szabályozás, mind a GDPR előírja

- Beletartozik a saját adatokba való betekintés

- Számos esetben az adatok feletti rendelkezés joga is

- Téves adatok helyesbítése

- Akár a törlés biztosításának joga is

Változások, kihívások

- 2008. USA: bűnözés > drog (105 mrdUSD)
- 106 nap (2017, Vectra Networks)
- 4 mrd netező, 10 mrd netes eszköz

IDC-ESET 2017. május:
- A vállalatok 22%-a nem ismeri a GDPR követelményeit
- 52% tud róla, de nem világos számukra a feladat
- A cégek ötöde (20%) még el sem kezdte a felkészülést
- A vállalatok 56%-nál nem mérik az adatlopások, támadások, kockázatok költségeit

IT-KIKÖTŐ 2017 GDPR-Adatvédelem újratöltve

Tanulópénzek

2008. UK NAVY

- 600,000 személyes adat

- egy állami alkalmazottól elloptak egy noteszgépet

BBC Home | Search

BBC NEWS | LIVE BBC NEWS CHANNEL

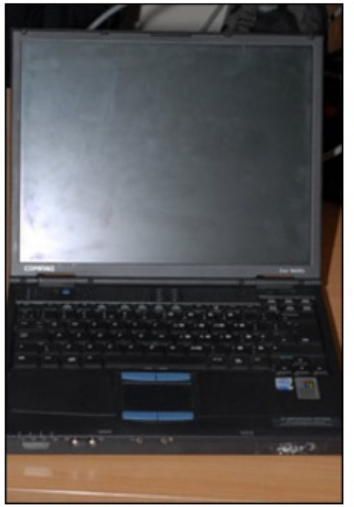
News Front Page
World
UK
England
Northern Ireland
Scotland
Wales
Business
Politics
Health
Education
Science & Environment
Technology
Entertainment
Also in the news
Video and Audio
Have Your Say
Magazine
In Pictures
Country Profiles
Special Reports
RELATED BBC SITES

Last Updated: Saturday, 19 January 2008, 18:41 GMT

E-mail this to a friend | Printable version

MoD to be quizzed over lost data

The information watchdog is to grill the Ministry of Defence over its data protection policies after it lost the personal details of 600,000 people.



The laptop, similar to the one in this picture, was stolen on 9 January

Defence Secretary Des Brown will also speak in the Commons next week about the latest loss of personal data, which went missing when a laptop was stolen.

The data includes passport and National Insurance numbers and bank details.

They relate to people who had expressed an interest in, or joined, the Royal Navy, Royal Marines and the RAF.

Information Commissioner Richard Thomas said the MoD laptop incident was "a stark illustration of the potency of personal information in a database world".

Tanulópénzek

2010. 280 ezer betegadat

- elvesztett adathordozón minősített, titkosítatlan adatok

DARKReading

Join us live at black hat INSECURITY

Authors Slideshows Video Tech Library University Radio Calendar Black Hat News

ANALYTICS | ATTACKS / BREACHES | APP SEC | CAREERS & PEOPLE | CLOUD | ENDPOINT | IoT | MOBILE | OPERATI

RISK

10/25/2010
04:34 PM

Personal Data Of 280,000 At Risk Following Healthcare Breach

Portable drive containing data on nearly 300,000 Medicaid patients in Pennsylvania is missing

Tim Wilson,
Editor in Chief,
Dark Reading
Quick Hits

0 COMMENTS
COMMENT NOW

Login

The personal data of nearly 300,000 Medicaid members is at risk following the loss of a storage device that contains their information, two healthcare providers said last week.

According to a news report, Keystone Mercy Health Plan and AmeriHealth Mercy Health Plan have reported the loss of a portable computer drive containing the names, addresses, and health information of 280,000 Medicaid members in Pennsylvania.

The affiliated companies together insure 400,000 people on medical assistance in Pennsylvania.

IT-KIKÖTŐ 2017 GDPR-Adatvédelem újratöltve

Tanulópénzek

2012.06. LinkedIn

- 6.5 millió account
- no salted hash
- több, mint 2 év
- 2FA, e-mail, kontroll

6.5 Million LinkedIn Passwords Reportedly Leaked, LinkedIn Is "Looking Into" It

Posted Jun 6, 2012 by Chris Velazco (@chrisvelazco)

If you're a LinkedIn user, do yourself a favor and change your password right now — according to a new report from Dagens IT, nearly 6.5 million encrypted LinkedIn passwords were recently dumped onto a Russian hacker forum.

The news comes right on the heels of yet another user security kerfuffle, as the most recent LinkedIn for iOS update was found to transmit users' meeting notes back to LinkedIn servers without their permission.

Of the millions of passwords dumped, Dagen IT claims that nearly 300,000 of them have been decrypted so far and that number seems sure to grow as users spread that hefty file around.

Crunchbase

LinkedIn

FOUNDED
2003

OVERVIEW
LinkedIn is a professional networking site that allows its members to create business connections, search for jobs, and find potential clients. The site also enables its users to build and engage with their professional networks; access shared knowledge and insights; and find business opportunities. It offers LinkedIn mobile applications across various platforms and languages such as iOS, Android, ...

LOCATION
Mountain View, CA

CATEGORIES

IT-KIKÖTŐ 2017 GDPR-Adatvédelem újratöltve

Tanulópénzek

2016.december: 90% XP a brit EÜ-ben

- nem várható érdemi javulás 2017-re

The Register®
Biting the hand that feeds IT

Software 160

90 per cent of the UK's NHS is STILL relying on Windows XP

And a load of them say they'll keep using it in 2017

By Gavin Clarke 8 Dec 2016 at 12:34 SHARE ▼

Accident and Emergency, the presumed location of many NHS IT folk. Pic: Shutterstock

The NHS is still running Windows XP en masse, two and a half years after Microsoft stopped delivering bug fixes and security updates.

Nearly all of England NHS trusts – 90 per cent – continue to rely on PCs installed with Microsoft's 15-year-old desktop operating system.

Just over half are still unsure as to when they will move to a replacement operating system.

Tanulópénzek

2017. július - Brit orvosok

- Snapchat-en küldik a röntgen képeket

- Tévhit, hogy a kényelmes egyenlő a jóval, vagy a biztonságossal

Why doctors using SnapChat to send scans is not the problem

06 JUL 2017 8

Google, Privacy, Security threats, Snapchat

by John E Dunn

Britain's vast, revered but increasingly troubled National Health Service (NHS) has many challenges to overcome but the one that is starting to really worry some sages is the way it uses – or more often fails to use securely – new technology.

As if a reminder of this perennial worry were needed, this week sees the publication of the first annual review from the Independent Review Panel, a body set up last year by Google's DeepMind Health (DMH) unit to report on the company's early work in the NHS.

Tanulópénzek

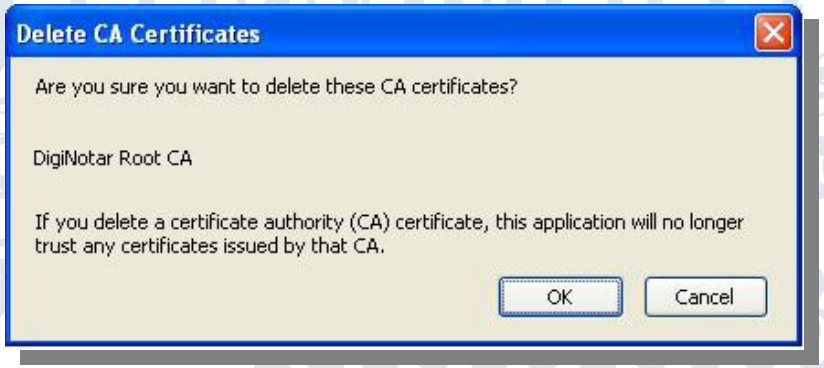
A titkolódzás súlyos és hosszú távon drágább hiba

- 2011. holland DigiNotar
- július 19-én nem csak feltörés áldozata
- a tanúsítványokat kibocsátó rendszerbe is bejutottak a támadók
- csak belső vizsgálat volt, nem értesítették a partnereket, a cég szerint „az incidens hatása minimális”
- A Comodo, a Google nevére kiállított illetéktelen tanúsítványok jelentek meg
- A kibocsátott hamis tanúsítványokat visszavonták (nem sokat ér), közben a Google.com-os kimaradt!
- Pl. az addons.mozilla.org-ra is állítottak ki tanúsítványt a támadók
- Az F-Secure kiderítette, hogy vélhetően iráni hackerek a diginotar.nl-t 2010-ben is többször megtörték, erről is hallgattak
- Független biztonsági jelentés:a behatoló már június 6-án bejutott a rendszerbe

Tanulópénzek

A titkolódzás súlyos és hosszú távon drágább hiba

- 531 tanúsítványt állítottak ki illetéktelenül, a tanúsító összes CA szerverét adminisztrátori szintig törték, és a logokat törölték
- a DigiNotarnak elképzelése sem lehetett arról, hogy kiknek a nevére generáltak így tanúsítványokat
- a DigiNotar július 19-éig mit sem tudott a dologról, és még szeptember 3-án is kiállításra kerültek új tanúsítványok
- **2011. szeptember 20. a DigiNotar (Vasco Inc. leányvállalata) belebukott a történetbe, felszámolás, csőd**



IT-KIKÖTŐ 2017 GDPR-Adatvédelem újratöltve

A szakma lehetséges feladatai

Milyen megoldásokkal segíthetjük a vállalkozásokat?

- ESET egy 30 éves gyártói tapasztalattal rendelkező cég
- A hálózati biztonság és végpontvédelem mellett további biztonsági technológiákkal
- A titkosítás és azonosítás mint az adatvédelmi megfelelés egyik eszköze

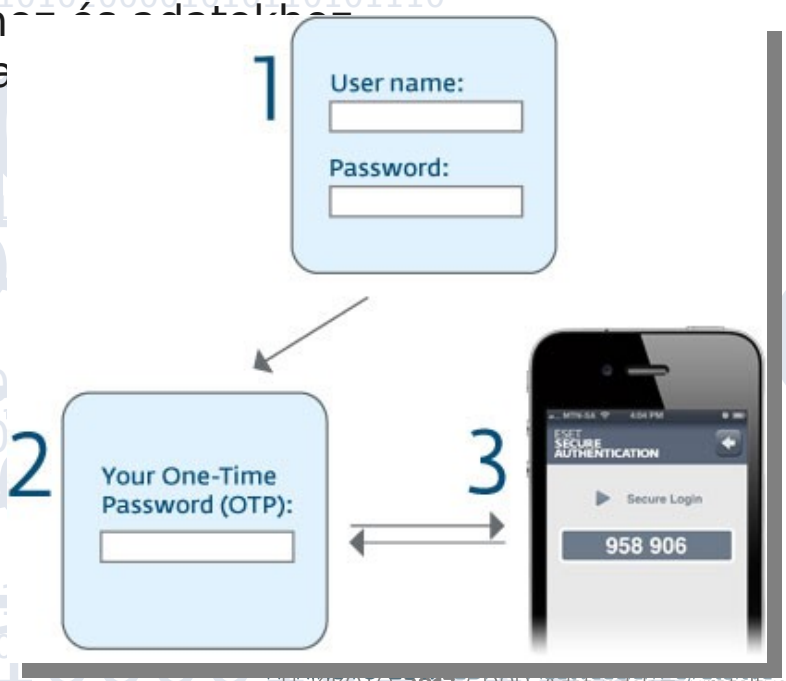
IT-KIKÖTŐ 2017 GDPR-Adatvédelem újratöltve

A szakma lehetséges feladatai

ESET Secure Authentication (ESA)

MIT OLD MEG?

- Problémamentes távoli hozzáférés céges hálózathoz és adatokhoz
- Erős mobil alapú megoldás, 2FA, egyszer használa
- Az OTP kód véletlenszerűen generált, nem megjósolható, nem újrahasználható
- Segíti a megfelelést az iparági szabályzásoknak (PCI-DSS/HIPAA)
- Az intézkedéssel demonstrálható a hozzáférési jogosultságok komolyan vétele
- Az adatvédelem melletti elkötelezettség (távoli hozzáférésnél)
- Jogosultságkezelési és naplózási kötelem előírása a szabályzás szerint



A szakma lehetséges feladatai

ESET Endpoint Encryption (DESlock Encryption)

MIT OLD MEG?

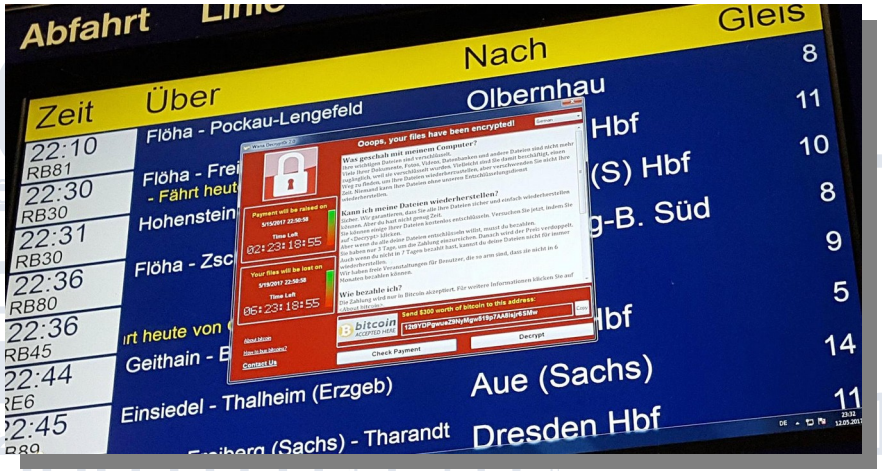
- Teljes HDD, cserélhető adathordozók, állományok, e-mailek titkosítása
- Szöveg és vágólap titkosítás
- Titkosított virtuális kötetek és tömörített állományok
- FIPS 140-2 szabványnak megfelelő
  256 bites AES titkosítás
- Szabványmegfelelés: COBIT, ITIL,
  ISO 27001, ISO 9001, ISO 14001
- bankkártyás fizetés (PCI DSS)
  szabvány kötelező eleme
- Skálázható, vállalati mérethez igazodó
- Menedzselt környezet, felhasználóbarát

- Az adatgyűjtés céljától eltérő adatkezelésnél kötelező a titkosítás

Biztonság+tudatosság

Biztonságtudatosság – ez is kell hozzá

2017. Global Cyber Risk
- 2016-ban sok helyen nem volt biztonságtudatossági képzés
- 46%-uknál ez évi egyszeri 30 perc
- 27% soha nem részesült oktatásban
- Megkerülhetetlenül fontos!



2017. május - WannaCry támadási hullám
- "Jó" apropó volt a cégek védekezésének felülvizsgálatára
- A brit dolgozók 44%: a céges levelezőrendszerben megnyitott e-mail biztonságos

IT-KIKÖTŐ 2017 GDPR-Adatvédelem újratöltve

Biztonság+tudatosság

Biztonságtudatosság – ez is kell hozzá

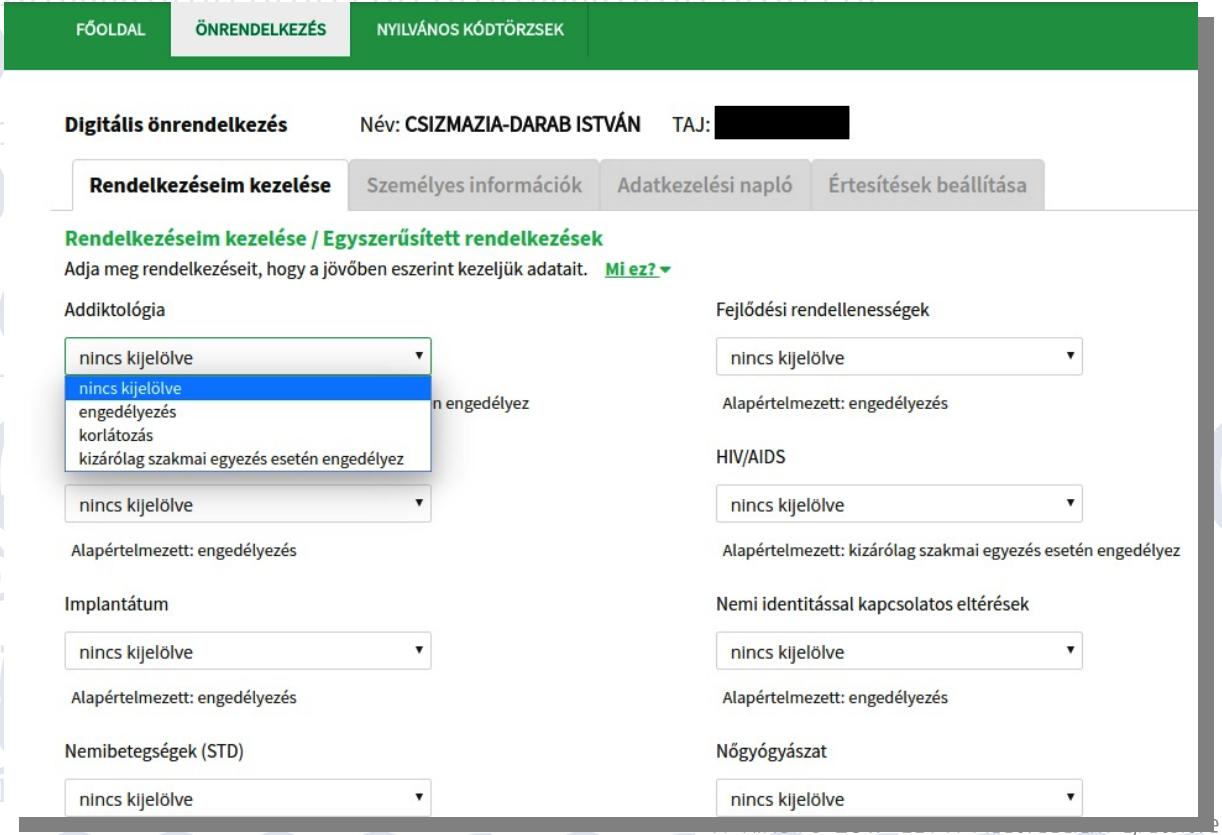
2011. december.
- Mi az indián neved?
- 800 ezer FB "kedvelő"
- még 2015-ben is 912 ezer

Biztonság+tudatosság

Biztonságtudatosság – ez is kell hozzá

Facebook – 2017.
„Ha 0-s a vércsoportod,
Különleges vagy! Ki még?”

Elektronikus Egészségügyi Szolgáltatási Tér (EESZT)
- Önrendelkezés: ki ismeri?



Biztonság+tudatosság

2014. Chimera:

- Nem várt mellékhatás: céges adatok Pastebin publikus weblapra

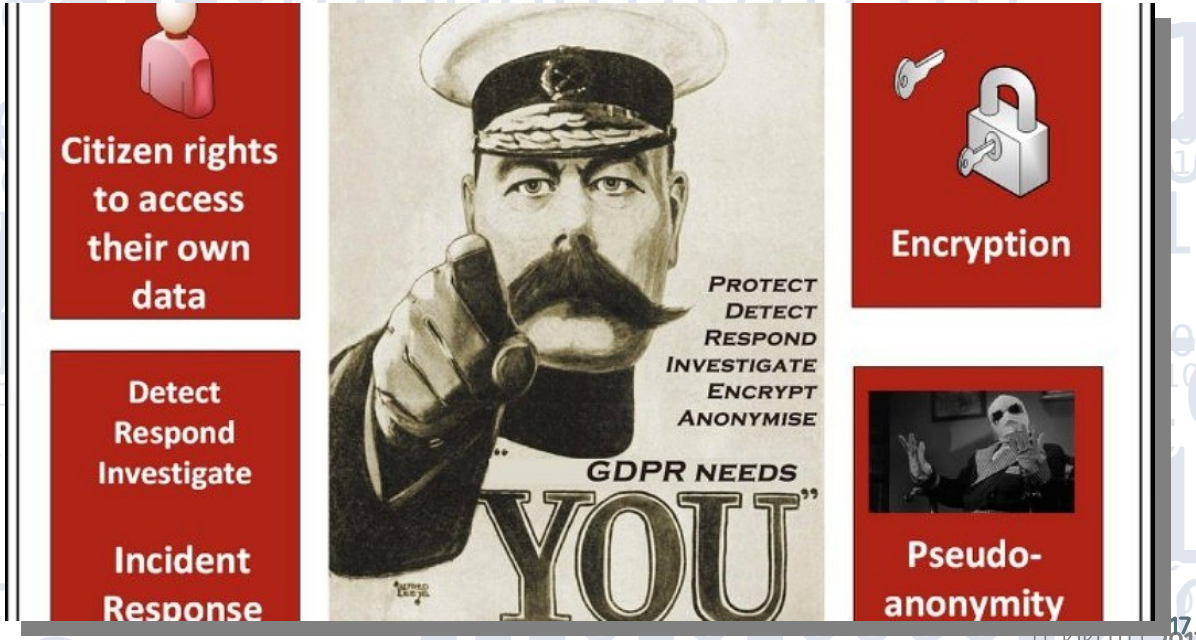
Várható lesz új bűnözői forgatókönyvek megjelenése:

- 20 mEUR helyett váltságdíj

IT-KIKÖTŐ 2017 GDPR-Adatvédelem újratöltve

Összefoglalva

- A cégek ötöde (20%) még el sem kezdte a felkészülést
- A felkészülés még a határidő után is rengeteg feladatot tartogat!
- Komoly változások, komoly bírságok
- A titkosítás és 2FA azonosítás az adatvédelmi megfelelés egyik eszköze
- Minden adatkezelőnek foglalkozni kell vele



Köszönöm a figyelmet!

Csizmazia Darab István
Sicontact, IT biztonsági szakértő