SAMARBEJDE OM CYBERSIKKERHED I FINANSBRANCHEN

Michael Busk-Jepsen
Finansrådet

AGENDA

1. Hvorfor taler alle om Cyber Security lige nu?
2. Cyber security - hvilke trusler er der i mod bankerne og bankernes kunder?
3. Hvad er hovedudfordringen?
4. Hvad samarbejder vi om i sektoren?

POLITICS

Obama to Announce Cybersecurity Plans in State of the Union Preview

By MICHAEL D. SHEAR JAN. 10, 2015

WASHINGTON — President Obama will announce new initiatives next week designed to bolster online security and improve access to cyberspace, White House officials said Saturday.

In a series of speeches, Mr. Obama will call for better safeguards against identity theft, improved privacy protection, enhanced cybersecurity for the government and private companies, and increased access to high-speed broadband connections across the country.

A White House official said in a statement to reporters that the president would "lay out a series of legislative proposals and executive actions that will be in his State of the Union that will tackle identity theft and privacy issues, cybersecurity, and access to the Internet."

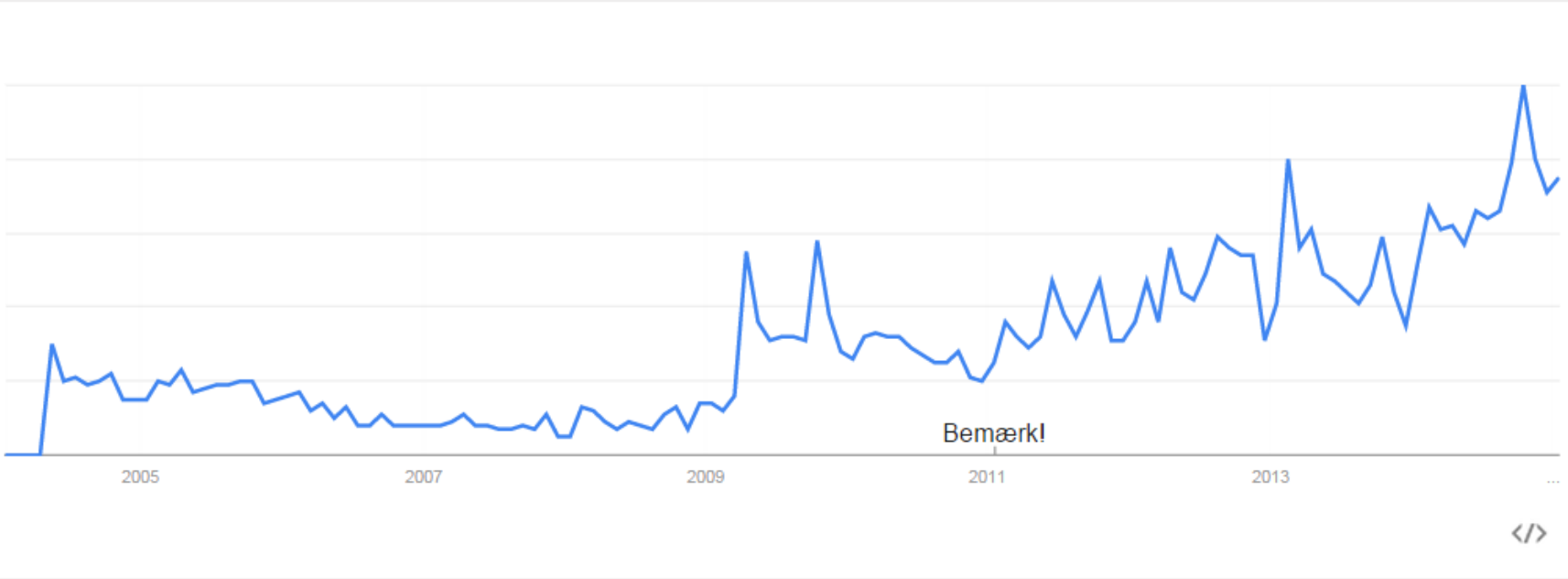
Google trend: Cybersecurity

"cybersecurity"
Søgeudtryk

+ Tilføj udtryk

Interesse over tid

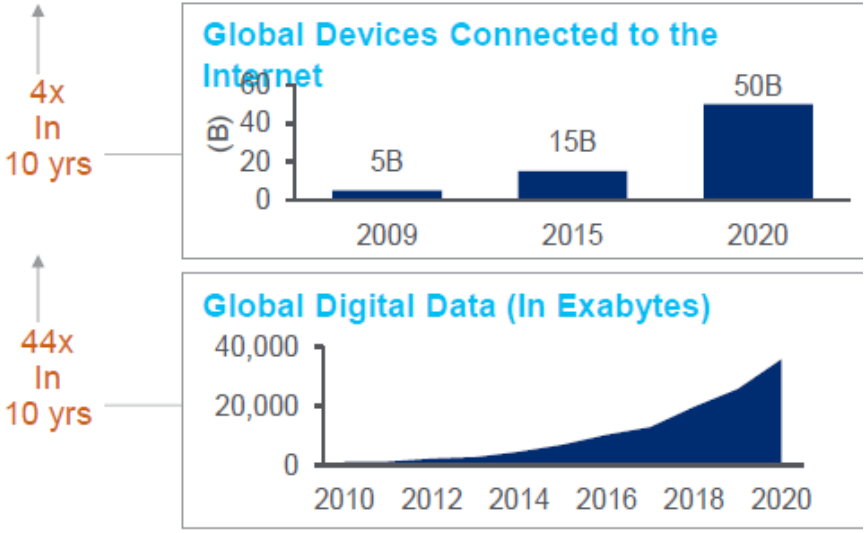
Nyhedsoverskrifter Prognose



1. HVORFOR TALER ALLE OM CYBER SECURITY LIGE NU?

Fordi transaktionerne flytter på nettet

Tremendous Growth of Online Interactions with each Click or Tap Leaving a Trail of Data



Kilde: Citi 2014

Netbank er blevet danskernes foretruk

00:55 11. jan 2015 | Af Berlingske Nyhedsbureau

Arkivfoto: Colourbox.

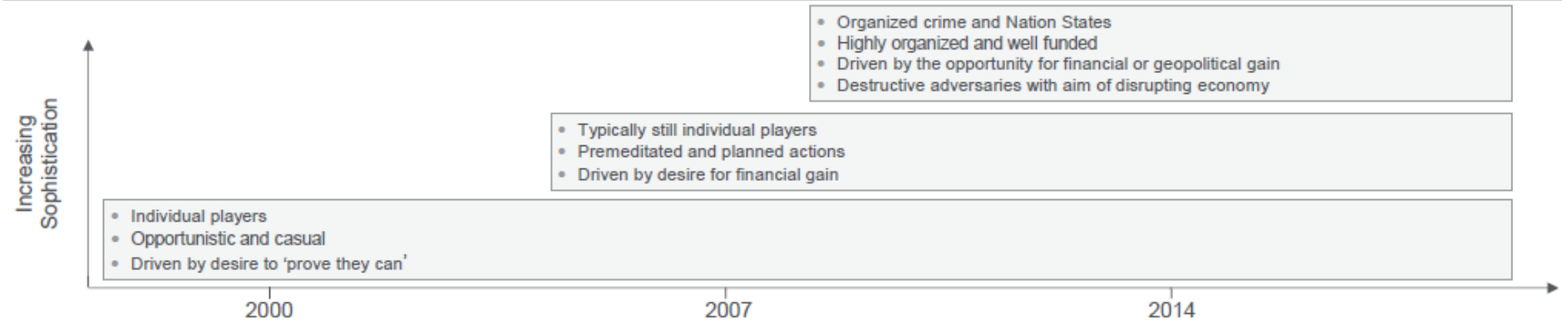
Den gode gamle bankmand er forvandlet til en portal på internettet.

Langt de fleste bankforretninger foregår i dag digitalt, og netbanken er på trods af forskellige mobile løsninger stadig hjørnestenen i bankforretninger for private og derfor meget vigtig for de fleste. Det fremgår af en endnu ikke offentliggjort BrancheIndex-undersøgelse, som er foretaget blandt 4.600 danske bankkunder. Det skriver Berlingske Business.

OG FORDI MODSTANDERNE ER BLEVET DYGTIGERE OG MERE SOFISTIKEREDE

The Changing Information Security Threat Landscape

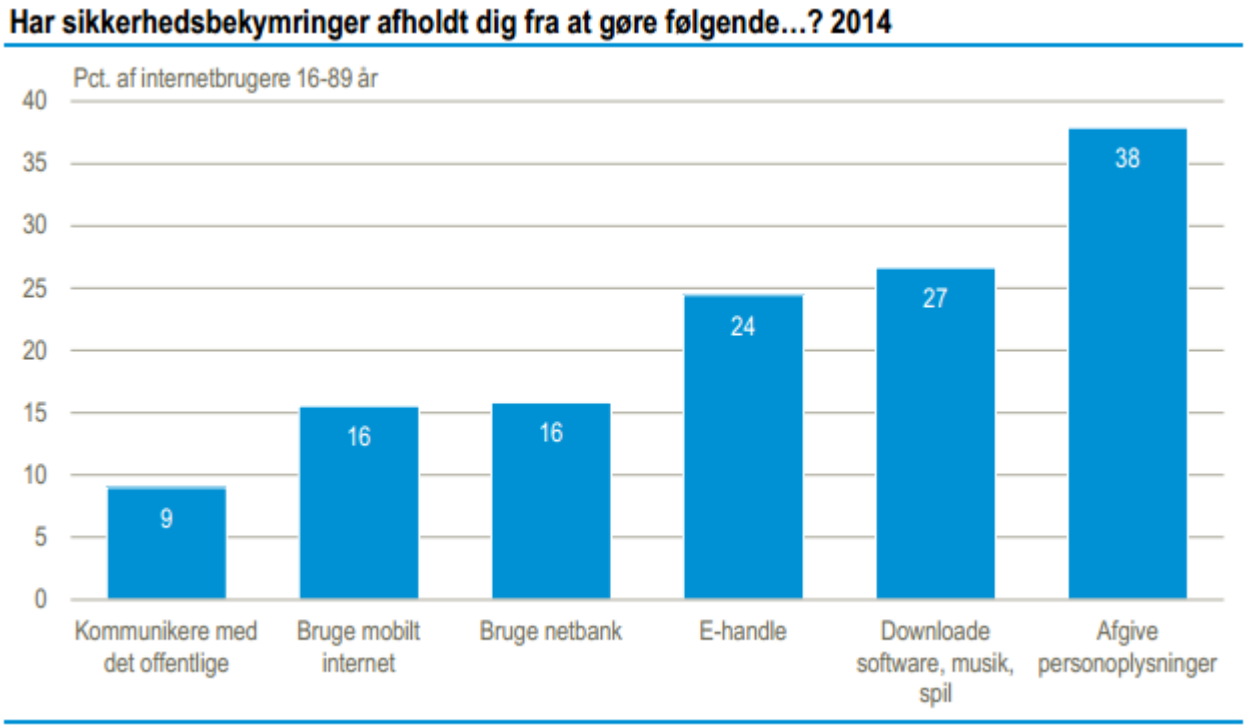
The cyber threat landscape continues to evolve as better organized and more sophisticated attackers have emerged.



Evolving Threats—An Illustration of the Information Security Challenge

	Past	Present
Speed of Attack	Non real-time theft of passwords and confidential information	Real time compromises of customer computers and communication channels
Target of Attack	Typically targets of opportunity	Frequently specifically chosen high value targets
Value of Information	Very variable—hard to monetize without exposing the malicious actor	Readily monetized in a sophisticated, secure, and anonymous underground economy
Complexity of Business Model	Workforce primarily based in same geography as business and on payroll	Workforce increasingly cross border and outsourced
Sophistication of Techniques	Moderately sophisticated adversaries seeking to exploit well known vulnerabilities	Highly sophisticated supply chain to create or detect vulnerabilities and exploit tools, then sold to "worker bees"
Availability of Tools	Custom tools created by knowledgeable individuals to perform a specific attack	Malicious tools are commodity items readily available on the black market

FORDI SIKKERHEDSBEKYMRINGER KAN AFHOLDE BRUGERNE FRA AT BENYTTE DE DIGITALE KANALER



Kilde: Danmarks Statistik, IT-anvendelse i befolkningen 2014

2. CYBER SECURITY - HVILKE TRUSLER ER DER I MOD BANKERNE OG BANKERNES KUNDER?

Eksempler på trusler for banker og kunderne

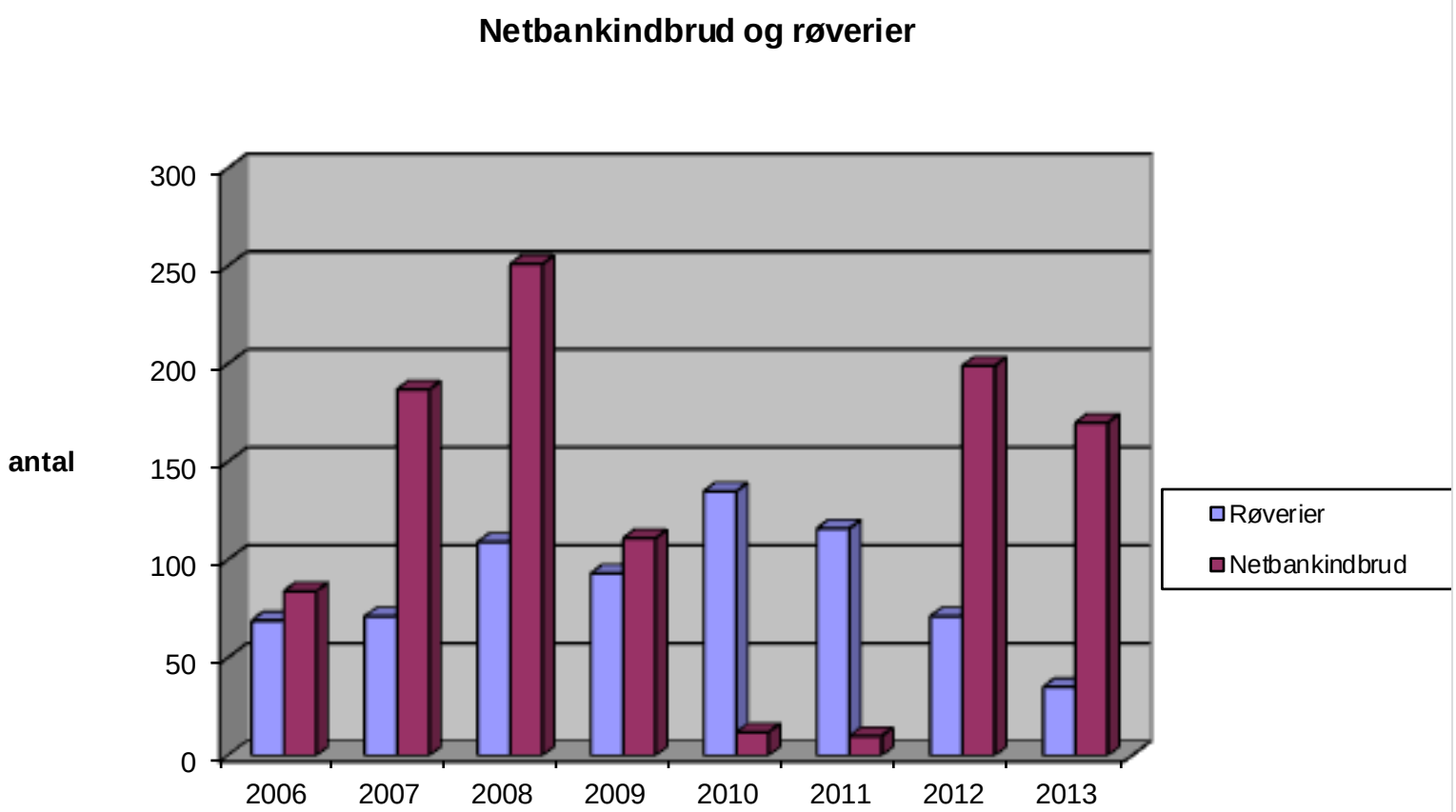
A. ”Simpel” berigelseskriminalitet

- Netbankindbrud
- Kreditkortsvindel
- Andre former for svindel

B. Eksponering/læk af personfølsomme oplysninger

C. Lukke infrastrukturen

A. Berigelseskriminaliteti DK:
- netbankindbrud og røverier



07. JAN. 2015 KL. 06:15 | OPDATERET 07. JAN. 2015 KL. 06:16

DR

Røvere går ikke længere i banken

Bankrøverier er snart historie. Siden 2010 er antallet af bankrøverier faldet med næsten 85 procent, viser nye tal fra Finansrådet.

A. Berigelseskriminalitet: netbankindbrud

NETTET 10. FEB. 2012 KL. 12.32

Netbankhackere bryder igennem NemId

Danske Bank-kunder har fået stjålet op mod 700.000 kroner af hackere.

DEL GEM TIL LISTE

SØREN DILLING
Journalist

MILLA MØLGAARD
Redaktør

Hackere har i otte tilfælde fået adgang til netbankkonti i Danske Bank og brudt NemID-sikkerheden undervejs, fremgår det af oplysninger fra selskabet Nets.

Ifølge en pressemeddelelse fra Nets har otte netbankkunder i de seneste dage været udsat for misbrug i netbanken.

Via såkaldt malware, som brugerne uforvarende er kommet til at installere på deres computere, har it-kriminelle haft mulighed for at udføre det, der med et teknisk udtryk kaldes "real time phishing".

Lignende sag hos Nordea

Misbruget har fundet sted, mens kunderne har været logget ind i deres netbank, oplyser Nets.

Netbankindbrud i DK

2014	1. kvartal	2. kvartal	3. kvartal	4. kvartal	I alt
Netbankindbrud	6	1	8	.	.
- Heraf med tab	4	1	7	.	.
Tabets størrelse i kroner	69.450	60.279	258.892	.	.

2013	1. kvartal	2. kvartal	3. kvartal	4. kvartal	I alt
Netbankindbrud	35	68	39	34	176
- Heraf med tab	14	26	13	17	70
Tabets størrelse i kroner	607.168,20	1.601.254,11	791.590,14	2.288.305,83	5.288.318,28

A: Berigelseskriminalitet, digital svindel

24. FEBRUAR 2014 15:21 AF: THOMAS VEIRUM THOMAS.VEIRUM@NORDJYSKE.DK

Fik nyt NemID med falske papirer

Københavns Politi afslører mulig sikkerhedsbrist

g+1 0 Tweet 0 Synes godt om 0

HELE LANDET: Tre mænd og en kvinde er mandag eftermiddag i grundlovsforhør ved Dommervagten i København. De er sigtet for at have bedraget sig til 70.000 kroner ved hjælp af NemID, skriver tv2.dk.

Ifølge tv2.dks oplysninger har en eller flere af de sigtede henvendt sig på Borgerservice med falske identitetspapirer, og med en undskyldning om at have glemt kodeordet, har vedkommende fået udstedt et nyt NemID.

Dermed er det ikke teknikken bag NemID, der har været problemet, men tilsyneladende den måde som NemID håndteres på Borgerservice.

Tømte bankkonti

Med det nye NemID i hånden har de sigtede angiveligt tømt bedrageriofferets bankkonti, og derefter vekslet beløbet til de såkaldte Bitcoins, der er en virtuel valuta.

Ring: 70263010
sigtet.dk
Forsvarsadvokat Gratis 24/7.

Hjørring cen
2-3 værelses ca.
kvm. m/opvasken
Leje fra 4.700-5.3
+ forbrug.
Tlf. 26 74 43

Søger rengørings
Tlf. 22 36 81

A: Berigelseskriminalitet, digital svindel med nye teknologier, ex: Mobile Pay

22. OKT. 2014 KL. 10:11 | OPDATERET 22. OKT. 2014 KL. 12:05

Politiet advarer: Mobilepay kan udnyttes af svindlere

Dankort-tyve og andre kriminelle kan udnytte populær betalingsapp fra Danske Bank til kortsvindel, lyder det.

Danske Banks mobilbetalingsløsning, Mobilepay, er sårbart overfor svindel, advarer politiet. © Colourbox

B. Læk af personfølsomme oplysninger
Ex: Se og Hør sagen

B. Læk af personfølsomme finansielle oplysninger. Ex: fra 2014: Home Depot, Target, Staples

Retailleddet:

- Home Depot (største DIY-kæde i USA): Den 18. september 2014 bekræftede Home Depot, at hackere havde fået adgang til 56 millioner betalingskortnumre.
- Target (supermarkedskæde med 1.800 butikker i USA): data (navne, kreditkortnumre) om 40 mio. amerikanere blev stjålet i november og december 2013.
- Staples (kontorudstyrskæde): kreditkortoplysninger fra mere end 1 mio. amerikanere stjålet.

Og også banker:

- JP Morgan fik i 2014 kompromitteret personoplysninger om kontorholdere af 83 mio. konti.

B. Eksempler på bankrelaterede angreb i 2014

(kilde: http://www.itgovernance.co.uk/blog/list-of-the-hacks-and-breaches-in-2014/

January

- 1 January, 2014 – 1.1 MILLION customers' credit card data was swiped in Neiman Marcus breach
- 20 January, 2014 – Credit Card Details of 20 Million South Koreans Stolen
- 25 January, 2014 – Michaels Stores confirms payment card information compromised in breach

February

- 24 February, 2014 – YouTube ads spread banking malware
- 25 February, 2014 – Mt. Gox exchange goes dark as allegations of $350 million hack swirl

March

- 14 March, 2014 – Credit Card Breach at California DMV
- 28 March, 2014 – Malware in 34 Spec's stores, payment data compromised for 550K

May

- 9 May, 2014 – WooThemes users notified of payment card breach, 300 reports of fraud

June

- 14 June, 2014 – P.F. Chang's Confirms Credit Card Breach
- 25 June, 2014 – European Bank Hit by Cyber Attack; £400,000 stolen

August

- 5 August, 2014 – Goodwill and FBI Investigate Possible Security Breach
- 15 August, 2014 – Supervalu supermarket chain begin investigating possible data breach
- 28 August, 2014 – FBI Probes Possible Hacking Incident at J.P. Morgan

September

- 4 September, 2014 – Home Depot suffers breach that may be larger than Target's
- 5 September, 2014 – 800k Payment Cards Compromised in Goodwill Industries Breach
- 18 September, 2014 – Home Depot: 56M Cards Impacted, Malware Contained
- 23 September, 2014 – 880,000 Affected by Viator Payment Card Breach
- 25 September, 2015 – Payment card data stolen in Jimmy John's data breach
- 30 September, 2014 – SuperValu compromised again – for the second time in three months
- **October**
- 3 October, 2014 – JPMorgan suffers data breach affecting 76 million customers
- 10 October, 2014 – Dairy Queen data breach hits 395 stores
- 21 October, 2014 – Staples stores investigated: suspected payment card breach

November

- 7 November, 2014 – Home Depot admits 53 million email addresses stolen in data breach
- 13 November, 2014 – Data breach affects 2.7 million HSBC Turkey cardholders
- 18 November, 2014 – Staples confirms POS malware attack

December

- 4 December, 2014 – Possible credit card breach at Bebe Stores
- 11 December, 2014 – Electronic payment company CHARGE Anywhere suffers five-year breach
- 22 December, 2014 – Staples confirm details of six-month breach, 1.16 million cards affected

C. Lukke infrastrukturen Ex: DDoS lukker forretningen

DDoS vil ske i fremtiden og infrastrukturen hærdes i forhold til det.

version2

Søg Søg

IT-NYHEDER | BLOGS | IT-JOB | IT-FIRMAER | WHITEPAPERS | Opret bruger | Log ind

EMNER *Digital signatur, It-sikkerhed, NemID*

Se kommentarer (31)

DDoS er nu hverdag for NemID: Nyt angreb trætter Nets

For femte gang på kort tid har NemID-appletten været udsat for DDoS-angreb. Tidskrævende at skulle håndtere nye angreb hele tiden, siger Nets DanID.

Af Mikkel Meister Torsdag, 18. april 2013 - 10:44

NemID blev onsdag aften ramt af endnu et DDoS-angreb, der gjorde det stort set umuligt for danskerne at logge på netbanken eller offentlige hjemmesider.

Det oplyser pressechef Søren Winge fra Nets:

»Vi oplevede et nyt angreb onsdag aften klokken cirka kvart i syv. Det er svært at sige præcist, hvornår det stoppede, men frem til klokken syv var der stor ustabilitet (på NemID-appletten, *red.*),« siger Søren Winge til Version2.

Som beskrevet på Version2 var der også problemer med ustabilitet onsdag eftermiddag, men da skyldtes det angiveligt de tekniske tiltag, som Nets DanID løbende arbejder på for at sikre NemID bedre mod DDoS-angrebene, der har hærget login-tjenesten den seneste uges tid.

Seneste nyt

Malware-ekspert: Her er et sikker netbank-login
16. sep 15.20

Micosoft må endnu en gang genudsende patches efter bøvl
16. sep 14.56

3. HVAD ER HOVEDUDFORDRINGERNE?

Dubex: *Hvad kan vi lære af 2014?)*

”2014 har på mange punkter været et skelsættende år for sikkerhedsindustrien.

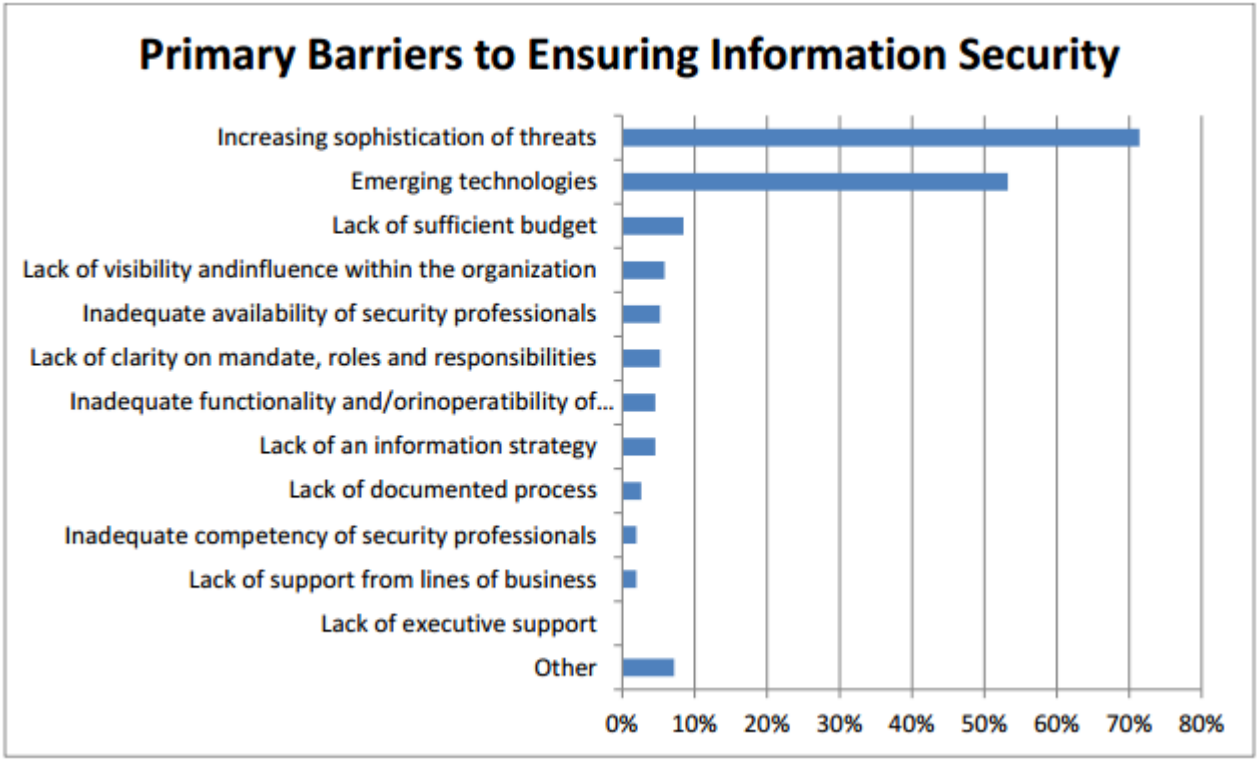
Cyberangrebene har nået et ikke tidligere set niveau målt på mængde, længde, kompleksitet og mål.

Og truslerne vokser fortsat og udvides til nye mål og områder. De tekniske angrebsmuligheder er mere mangfoldige end nogensinde, og hackere kombinerer metoderne på nye og skræmmende måder.

Selv organisationer med godt styr på sikkerheden er ofre for succesfulde angreb.”

(Kilde: Dubex, *Hvad kan vi lære af 2014?)*

Vilkår: nye teknologier, nye trusler



Kilde:

New York State, Department of Financial Services, Report on Cyber Security in the Banking Sector

Governor Andrew M. Cuomo, Superintendent Benjamin M. Lawsky, Maj 2014

Vilkår: Nye aktører

Cyber Criminals

Motivation: Make Money.

Methods: Very mature underground economy supporting every facet of cyber criminal activity.

Cyber Terrorism

Motivation: Instill fear so targets comply with demands or ideology.

Methods: Using cyber to "enable" their programs (Recruit, Incite, Train, Plan and Finance). Underground forums allow these groups to easily acquire destructive capabilities.

Hactivists

Motivation: Seek publicity for their geopolitical agenda.

Methods: Disruption and Defacement.

State-Affiliated (Advanced Persistent Threat)

Motivation: Political and technological advantage to improve self interests.

Methods: Advanced operations to gain a foothold into a target's infrastructure. Once a foothold is established, the adversary performs reconnaissance and methodically plans their attack. APT actors often leave back doors to re-establish access to the target in case their primary means is identified and mitigated.

4. HVAD SAMARBEJDER VI OM I FINANSSEKTOREN?

Vi gør allerede meget (regulering)

Der findes allerede en meget omfattende regulering og tilsyn med finansielle virksomheder i forhold til it-sikkerhed:

- persondataloven,
- lov om finansielle virksomheder,
- lov om betalingstjenester og elektroniske penge,
- bekendtgørelse om ledelse og styring af pengeinstitutter m.fl.,
- bekendtgørelse om outsourcing af væsentlige aktivitetsområder,
- bekendtgørelse om systemrevisionens gennemførelse i fælles datacentraler og
- bekendtgørelse om revisionens gennemførelse i finansielle virksomheder mv. samt finansielle koncerner.

Reguleringen efterleves individuelt af den enkelte bank i dag.

Vi gør allerede meget (sektorsamarbejde)

Eksempler på eksisterende sektorsamarbejde om it-sikkerhed

- IT-sikkerhedsforum
- Sektorfælles kontrakt med en ekstern sikkerhedsleverandør
- Samarbejdsudvalget for kort- og netbankmisbrug
- NemID-koordinationsudvalg
- Aftale med GovCERT
- Deltager i div off. fora: Strategisk samarbejdsforum for cybersikkerhed, Forum for identitetstyveri
- Intranationalt : EBF IT-fraud task force, EU FI ISAC, Nordic eBanking Security Summit m.v.

Og vi kommer til at gøre endnu mere

- *styrke de enkelte bankers muligheder for at håndtere cyber- og it-sikkerhedstrusler*
- *styrke sektorsamarbejdet og handlemulighederne i sektoren i forhold til cyber- og it-sikkerhedstrusler både nationalt og internationalt*
- *styrke samarbejdet med det offentlige og med andre interesseorganisationer*
- *bidrage til at sikre, at borgerne har den nødvendige viden om it-sikkerhed*
- *bidrage til at styrke især mindre virksomheders muligheder for at beskytte sig imod cyber- og it-sikkerheds-trusler.*

SPØRGSMÅL ELLER KOMMENTARER