5. DATAGOVERNANCE: SIKKERHED OG PRIVACY

START MED EN HISTORIE

Exposition

Den 12. maj 2017 forekom det højeste niveau af ransomware-angreb, der blev målrettet over hele verden. Ransomware anvendte udnyttelse kaldet EternalBlue, en sårbarhed, der drives af NSA og frigivet til offentligheden af ShadowBrokers.

Når en computer var inficeret med WannaCry, krypterede den alle data. Programmet satte op en skærm, der krævede løsepenge i form af virtuel Bitcoin for at få tilbage adgang, med løsepenge stigende over tid indtil slutningen af nedtællingen, hvor alle filerne ville blive ødelagt.

Wannacry påvirkede mere end 200.000 systemer fra virksomheder, offentlige agenturer og enkeltpersoner i mere end 150 lande. Større organisationer som National Health Services (NHS) [1] i Storbritannien og Renault-Nissan måtte stoppe produktionen i nogle områder som et resultat. En række store virksomheder blev også berørt, herunder Telefonica, FedEx, Deutsche Bahn, Santander og KPMG.

Hvorfor var dette angreb så potent?

- For det første, hvordan det spredte sig. Den mest almindelige infektionsrute for konventionel Ransomware var ved at sprede sig via phishing-e-mail og besøge et websted. Ransomware blev distribueret som en mail for at opmuntre brugerne til at klikke på e-mail-vedhæftede filer eller hacke sig ind på en webserver og være forklædt som en annonce, så når en bruger besøger hjemmesiden, bliver bruger-pc'en inficeret. Imidlertid havde WannaCry ransomware egenskaber ved en orm, der distribueres autonomt gennem netværket uden nogen brugerhandling. Hver Windows-computer uden patch var sårbar over for infektionen.

- For det andet ubeskyttede operativsystemer. En af de største bidragydere var, at et stort antal computere ikke havde Microsofts patch installeret eller kørte versioner af Windows, som der ikke var nogen patch til.

Erfaringer

Ledere kunne ikke erkende, at de for at afskrække og minimere potentialet ved cyberangreb er nødt til at sikre, at deres operativsystemer konstant opdateres og lappes på tværs af alle netværk.

EXPOSITION

1. DATA SIKKERHED

Eksperter advarer om, at WannaCry bare var begyndelsen, og tallene bekræfter dette synspunkt.

Blandt små virksomhedsejere hersker den uheldige misforståelse, at hackere kun er interesseret i at angribe store virksomheder. Faktum er, at hackere elsker SMV'er. Disse mindre virksomheder fokuserer mindre på sikkerhed og har ikke de IT-sikkerhedsbudgetter, som store virksomheder har. har ikke midler til at betale for sikkerhedsanalytikere eller intern it. [2]

Typer af trusler

[1] https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyberattack-cio-review.pdf

[2] https://www.telegraph.co.uk/business/cybersecurity-for-small-business/fraud-prevention/

En dataovertrædelse er en hændelse, hvor der er adgang til følsomme eller på anden måde beskyttede oplysninger uden tilladelse. Det kan dræne de magre ressourcer, som SMV'er har, og formindske forbrugertilliden. Kort sagt, manglende sikkerhed kan slå dig konkurs.

2. DATA PRIVACY

Hvorfor betyder privatliv?

1. Begrænsning af strømmen. Privatlivets fred er en grænse for regeringens magt såvel som den private sektors virksomheders magt. Jo mere nogen ved om os, jo mere magt kan de have over os. Personlige data bruges til at tage meget vigtige beslutninger i vores liv. Personlige data kan bruges til at påvirke vores omdømme; og det kan bruges til at påvirke vores beslutninger og forme vores opførsel. Det kan bruges som et værktøj til at udøve kontrol over os. Og i de forkerte hænder kan personoplysninger bruges til at forårsage os stor skade. [3]

2 friheder. Privatliv er nøglen til tanke- og ytringsfrihed og hjælper med at beskytte vores evne til at omgås andre mennesker. En vigtig komponent i foreningsfriheden er evnen til at gøre det med privatlivets fred, hvis man vælger det. Privatliv er en kritisk komponent i et demokratisk samfund.

3. Rettigheder til en anden chance Mange mennesker er ikke statiske; de ændrer sig og vokser gennem hele deres liv. Der er en stor værdi i evnen til at have en anden chance, at være i stand til at bevæge sig ud over en fejltagelse, at være i stand til at genopfinde sig selv. Privatliv nærer denne mulighed. Det giver folk mulighed for at vokse og modne uden at være bundet af alle de tåbelige ting, de muligvis har gjort i fortiden

Databeskyttelse er forskellig fra databeskyttelse

- Privatliv er et kompliceret spørgsmål, der vedrører rettigheder og friheder, der er nedfældet i henhold til loven. Databeskyttelse er forskellig fra databeskyttelse. Beskyttelse handler om at sikre data mod uautoriseret adgang. Datapolitik handler om autoriseret adgang - hvem der har det, og hvem der definerer det. Databeskyttelse er i det væsentlige et teknisk problem, mens databeskyttelse er et lovligt.
- Teknologi alene kan ikke sikre privatlivets fred for personlige data. De fleste beskyttelsesprotokoller er stadig sårbare over for autoriserede personer, der muligvis får adgang til dataene. Byrden for disse autoriserede personer handler først og fremmest om privatlivets fred og ikke teknologi.

BNPR

- GDPR er en regulering i EU-lovgivningen om databeskyttelse og privatliv for alle individuelle borgere i Den Europæiske Union (EU) og Det Europæiske Økonomiske Samarbejdsområde (EØS). Den vedrører også overførsel af personoplysninger uden for EU og EØS-områder. [4]
- Det er målet at holde virksomheder ansvarlige for at beskytte de personlige data, der i stigende grad fejes op i dagens digitale verden
- Det henhører under de nationale tilsynsmyndigheder - i Storbritannien, informationskommissærens kontor - at håndhæve reglerne for virksomheder inden for deres jurisdiktion.
- Sanktioner: I henhold til GDPR kan regulatorer bøde et firma så meget som 4% af det årlige salg, selvom de fleste bøder hidtil har været langt mindre, typisk mindre end $ 1 million.

Personlige oplysninger skal være:

- behandles lovligt, retfærdigt og gennemsigtigt ('lovlighed, retfærdighed og gennemsigtighed');
- indsamlet til specificerede, eksplicitte og legitime formål og ikke viderebehandlet på en måde, der er uforenelig med disse formål; ('formålsbegrænsning');
- tilstrækkelig, relevant og begrænset til, hvad der er nødvendigt i forhold til de formål, de behandles til ('dataminimering');

---

[3] https://teachprivacy.com/10-reasons-privacy-matters/

[4] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

- nøjagtig og om nødvendigt opdateret ('nøjagtighed');
- opbevares i en form, der tillader identifikation af registrerede ikke længere end nødvendigt til de formål, som personoplysningerne behandles til ('opbevaringsbegrænsning');
- behandles på en måde, der sikrer passende sikkerhed for personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod utilsigtet tab, ødelæggelse eller skade, ved hjælp af passende tekniske eller organisatoriske foranstaltninger ('integritet og fortrolighed').

British Airways casestudie

- En halv million passagerrekorder blev adgang i et cyberangreb mellem 21 st August og 5 th september 2018. Virksomheden løste overtrædelsen af sit websted og app den 6. th September og politiet blev underrettet.

- Informationskommissærens kontor (ICO) oplyste, at en række informationer blev kompromitteret af dårlige sikkerhedsordninger, herunder login, betalingskort og rejsebestillingsoplysninger samt oplysninger om navn og adresse.

- Flyselskabet bliver nødt til at betale 183,39 mio. Pund (230 mio. Dollars) til ICO for ikke at beskytte sine kunders data, den største straf, der er indledt af nationale tilsynsregler for privatlivets fred i hele EU siden vedtagelsen af GDPR. [5]

3. DATAETIK

Datakraften er så stor og kan have en så stor effekt på vores liv, at vi ikke burde forestille os data som Is og Os, men som en digital sjæl. Begrebet "digital sjæl" blev beskrevet som den elektroniske repræsentation af dig selv. At skabe en model for ejerskab og kontrol af denne idé er den store udfordring for virksomheder, der besidder data, såvel som enkeltpersoner og regulatorer

Lessigs patetiske prik

Den patetiske dotteori eller New Chicago School teorien blev introduceret af Lawrence Lessig i en artikel fra 1998 og populariseret i hans bog fra 1999, *Kode og andre love inden for cyberspace*. Det er en socioøkonomisk teori om regulering. [6] Den diskuterer, hvordan enkeltindividers liv (de patetiske prikker i spørgsmål) reguleres af fire kræfter: loven, sociale normer, markedet og arkitektur (teknisk infrastruktur).

Teorien fremhæver, hvordan computerkode kun er en af de regulatoriske betingelser, der kan ændre adfærd, og derfor er forståelse af andre mekanismer som loven, normerne og etikken afgørende for at opbygge teknologier, der ikke resulterer i uønsket adfærd.

Dataetik handler om at gå ud over lovgivningen og forstå, hvordan markeder, normer og kode interagerer for at sikre, at vi er etiske i vores brug af den enkeltes data. Vi skal gå ud over overholdelse til at bruge data på den bedst mulige måde for alle involverede.

Tre store temaer Samtykke. Samtykke er det, som mange mennesker diskuterer, når de tænker på teknologietik. Under GDPR er kravene om samtykke blevet styrket for at kræve en positiv og utvetydig handling for at "vælge". Det er ikke længere en engangsbeslutning, men et igangværende spørgsmål, der skal omhyggeligt

[5] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-britishairways/

[6] https://en.wikipedia.org/wiki/Pathetic_dot_theory

overvåges. Enkeltpersoner kan til enhver tid trække deres samtykke tilbage uden straf. Mekanismerne for tilbagetrækning af samtykke skal være lige så lette som dem til at give samtykke. Enkeltpersoner skal have et ægte valg om, hvorvidt de samtykker eller ej. Hvis de ikke har et valg, anses samtykke ikke for at være givet frit og vil ikke være gyldigt.

Datadeling . Stærk etisk praksis og risikobegrænsende praksis udelukker deling af data uden samtykke fra de mennesker, der afslører dem. De udelukker også at dele data med parter, som der ikke er givet adgang til. Men effektiv brug af data kræver, at de deles - og især i den digitale erhvervstid med en voksende platformøkonomi. Flere og flere organisationer samarbejder om at skabe nye tilbud og endda nye brancher. Disse samarbejder kræver udbredt og konstant datadeling, hvilket bringer nye og vanskelige at forudsige risici. Disse risici forværres af det faktum, at når datasæt når en stor nok størrelse, er anonymitet en myte.[6] Og når yderligere datasæt er samlet, kan enkeltpersoner identificeres med relativ lethed.[7], [8] Adressering af problemer og skader, der er forbundet med deling data, [7])

Algoritmisk ansvarlighed og bias. Måder, hvor klassificeringsalgoritmer kan tilpasses eller evalueres for at mindske potentielle bias eller gennemsigtighedsproblemer. I årevis har snesevis af rapporter fra organisationer som ProPublica afsløret omfanget af algoritmisk forskelsbehandling i vurdering af kriminel risiko , forudsigelig politiarbejde , kreditudlån , leje , og mere. Bias kan være et menneskeligt problem, men *amplifikation* af bias er et teknisk problem - et matematisk forklarbart og kontrollerbart biprodukt af den måde, modeller modeller trænes på.

Bare fordi en algoritme er fair, betyder det ikke, at den bruges retfærdigt . Praktikanter skal tage skridt ved nøje at gennemgå algoritmiske tilgange til afhjælpning af bias. Det er vores ansvar at kritisk forhøre, hvem der drager fordel af disse teknologier til hvis omkostninger, og at være vokale om, hvordan vores modeller skal eller ikke skal bruges.

Eksempler på algoritmisk bias

Ansigtsgenkendelsessoftware bruges i stigende grad i retshåndhævelse - og er en anden potentiel kilde til både race og kønsfordeling . I februar i år fandt Joy Buolamwini ved Massachusetts Institute of Technology, at tre af de nyeste kønsgenkendelses AI'er, fra IBM Microsoft og det kinesiske firma Megvii, korrekt kunne identificere en persons køn fra et fotografi 99 procent af tiden - men kun til hvide mænd. For mørkhudede kvinder, nøjagtighed faldt til kun 35 procent . Det øger risikoen for forkert identifikation af kvinder og mindretal. Igen er det sandsynligvis ned til de data, som algoritmerne trænes på: hvis den indeholder mere hvide mænd end sorte kvinder, vil det være bedre til at identificere hvide mænd. IBM annoncerede hurtigt, at det havde omskoleret sit system på et nyt datasæt, og Microsoft sagde, at det har taget skridt til at forbedre nøjagtigheden. Kilde: New Scientist: https://www.newscientist.com/article/216620

4. INFORMATIONSSTYRING

Dataovertrædelser er alvorlige, og kunderne selv kræver stadig bedre opmærksomhed på datahetik, så vi er nødt til at tage datastyring alvorligt. Virksomheder har brug for en nødplan, men forebyggelse er bedre end kur.

Der er ingen løsning i én størrelse, der passer til alle.

---

7 https://www.accenture.com/_acnmedia/pdf-22/accenture-data-ethics-pov-web.pdf

Definition: "... specifikation af beslutningsrettigheder og en ansvarlighedsramme for at tilskynde til ønskelig adfærd ved værdiansættelse, oprettelse, opbevaring, brug, arkivering og sletning af information." (Logan, 2010). Ordreord indeholder det et sæt regler og vejledning til, hvordan data eller information håndteres i en organisation. (Citeret i Rising, Kristensen, Tjerrild-Hansen, 2014 [8])

Mål

1. maksimere værdien af information til organisationen ved at sikre, at informationen er pålidelig, sikker og tilgængelig til beslutningstagning
2. beskytte information, så dens værdi for organisationen ikke formindskes ved hjælp af teknologi eller menneskelig fejl, tab af rettidig adgang, upassende brug eller fejlagtig fejl.

Hvorfor er det informationsstyring og ikke datastyring?

”Kort sagt henviser data til rå, uorganiserede fakta. Tænk på data som bundter af masseposter indsamlet og gemt uden kontekst. Når kontekst er blevet tilskrevet dataene ved at strenge to eller flere stykker sammen på en meningsfuld måde, bliver det information. ” Lebanthal

4 Risikovurdering

En risikovurdering hjælper dig med at forstå de områder, du har brug for at beskytte, de områder, hvor du kunne være mest sårbar og potentielle worst-case scenarier. Start med at kontrollere de data og oplysninger, du har, som er mest værdifulde. Se derefter på, hvordan du gemmer disse data, hvem der har adgang til dem, og hvordan de er beskyttet af teknologi og processer for at forstå, hvor du kan være mest udsat for. Hvis du ikke er sikker på at udføre en risikovurdering, kan du overveje at ansætte en ekspert til at gøre dette for dig.

En effektiv responsplan skal omfatte følgende elementer:

- Dit juridiske svar: Du skal skitsere, hvordan du håndterer de juridiske aspekter af overtrædelsen, for eksempel at informere Informationskommissærens kontor (ICO) om problemet og forsvare din virksomhed mod ethvert krav om uagtsomhed.
- Håndtering af medieforespørgsler: Din virksomhed kan være fokus for medieopmerksomhed efter et brud, så vær klar til at håndtere al ekstern kommunikation om, hvad der skete, og hvordan du håndterer det. Du har sandsynligvis brug for professionel PR-ekspertise for at gøre dette effektivt.
- Find ud af, hvad der skete: Du bliver også nødt til at have it-kriminaltekniske eksperter til rådighed for at finde ud af, hvad der har forårsaget overtrædelsen, med henblik på hurtigt at afhjælpe problemet og sikre, at det ikke sker igen.

- Informere kunder: Afhængigt af dit kundebase og omfanget af overtrædelsen, kan du have en masse ubehagelige telefonopkald at foretage! Du skal være klar med en måde at håndtere denne kommunikation på effektivt.

BEMÆRK TIL

Cyberforsikring

Hvis du står overfor følgevirkninger af et dataovertrædelse , din sidste forsvarslinie er en vandtæt og specialis t cyberforsikring . Dækker dig for overtrædelse af lovgivningen om databeskyttelse (hvor det er forsikringsmæssigt lovligt) og dit ansvar for håndtering af data, kan det også give dækning for afpresning, omkostninger til systemudligning, plus PR-udgifter og økonomisk tab på grund af systemstop.

Nogle vigtige aspekter, man skal kigge efter inkluderer:

- Informationskommissærens kontor (ICO) kan give bøder på op til £ 500.000 for overtrædelse af databeskyttelsesloven. Cyber-forsikringspolitikken med digital risiko dækker anmeldelseomkostninger,

8 https://web.stanford.edu/class/msande238/projects/2014/GainIT.pdf

juridiske gebyrer, der forsvarer lovgivningsmæssige handlinger, og i nogle tilfælde selve sanktionen (hvor dette lovligt kan forsikres).

- Dæk for dine udgifter til lommer, som kan omfatte udgifter til systemreparation, tabt indkomst, mens systemet er nede, eller endda løsgift til hackere.
- Dækning til dit websted, blogs og sociale medier, til krænkelse af copyright eller varemærke eller ærekrænkelse osv.

Casestudier

GENERATION DATA

USING DATA FOR PROFIT

Facebook Social S ikkerhed Casestudie

CYBERNET SIKKERHEDSCENTER UNDER FORSVARINGSMINISTERIET

FACEBOOK SOCIAL SIKKERHED

Hvorfor kan din personlige konto være nyttig?

- For personlige oplysninger om dig:

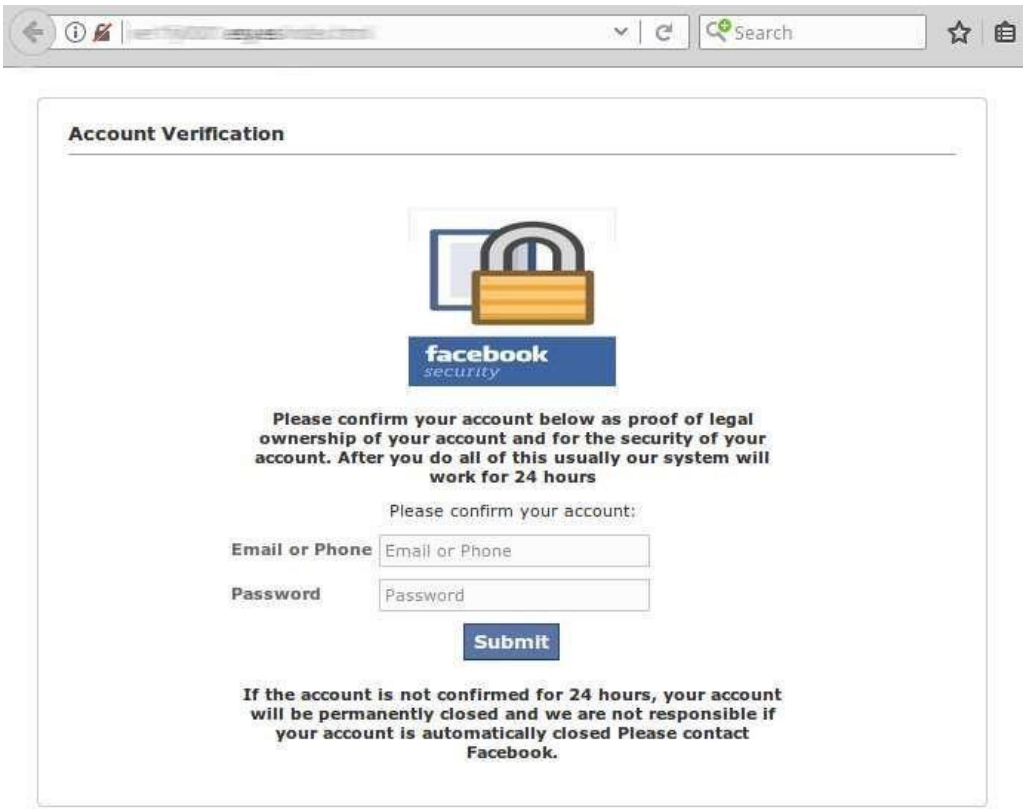
o Kontakter; o billeder; o andre personlige oplysninger (når du rejste, hvor du rejste, hvor du bor, betalte, arbejde, hobbyer, hobbyer osv.);

- For information om de mennesker, du kommunikerer med;
- Forfalskninger af sider, kommentarer osv .;
- For Facebook-grupper og sider administreret af din konto.

Der lægges særlig vægt på Facebook-grupper, sider og enkeltpersoner - især dem, der har et betydeligt antal følgere. Stålne Facebook-sider og konti sælges ondsindet til tredjepart, udnyttet til reklame og andre formål.

Hvordan kapres Facebook-konti?

- Mest stjålne adgangskodebeskyttede konti;
- Login-detaljer kommer fra andre kilder (e-mail, andre online-konti); • Loginoplysninger indsamles på offentlige enheder og offentligt tilgængelige gratis trådløse netværk (gratis wifi);
- Login stjålet gennem social engineering (ved at sende falske e-mails med links til Facebook phishing)



Figur 1. Et eksempel på social ingeniørarbejde er forfalskning af sider

Ansvar for uautoriseret login til din Facebook-konto.

Ansvaret for sådanne aktiviteter er beskrevet i artikel 198 1, stk. 1, og 198 2, stk. 1, i Republikken Litauens straffelov.

Artikel 198 1. Ulovlig adgang til informationssystem

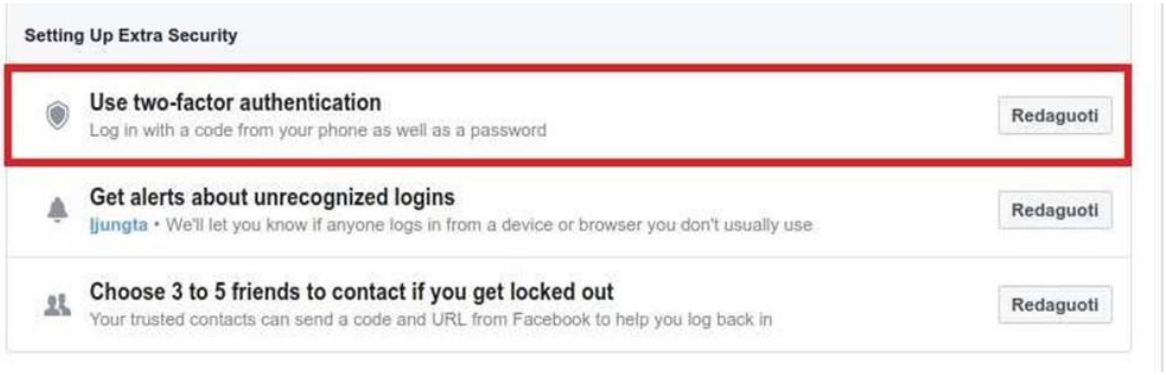
Den, der ulovligt har adgang til informationssystemet eller en del af det i strid med informationssystemets sikkerhedsforanstaltninger, der kan straffes med offentlige arbejder eller bøder, eller anholdelse eller fængsel i op til to år.

Artikel 198 2. Uautoriseret bortskaffelse af enheder, software, adgangskoder, koder og andre data

Enhver, der til kriminelle formål eller på anden måde har produceret, transporteret, importeret, solgt, gjort tilgængeligt eller på anden måde distribueret, erhvervet eller besiddet enheder eller software, der direkte er beregnet eller tilpasset til at begå forbrydelser, samt adgangskoder, koder eller andre lignende data til logning videre til et informationssystem eller en del deraf, der kan straffes med offentlige arbejder eller med bøde, eller med anholdelse eller fængsel i op til tre år.

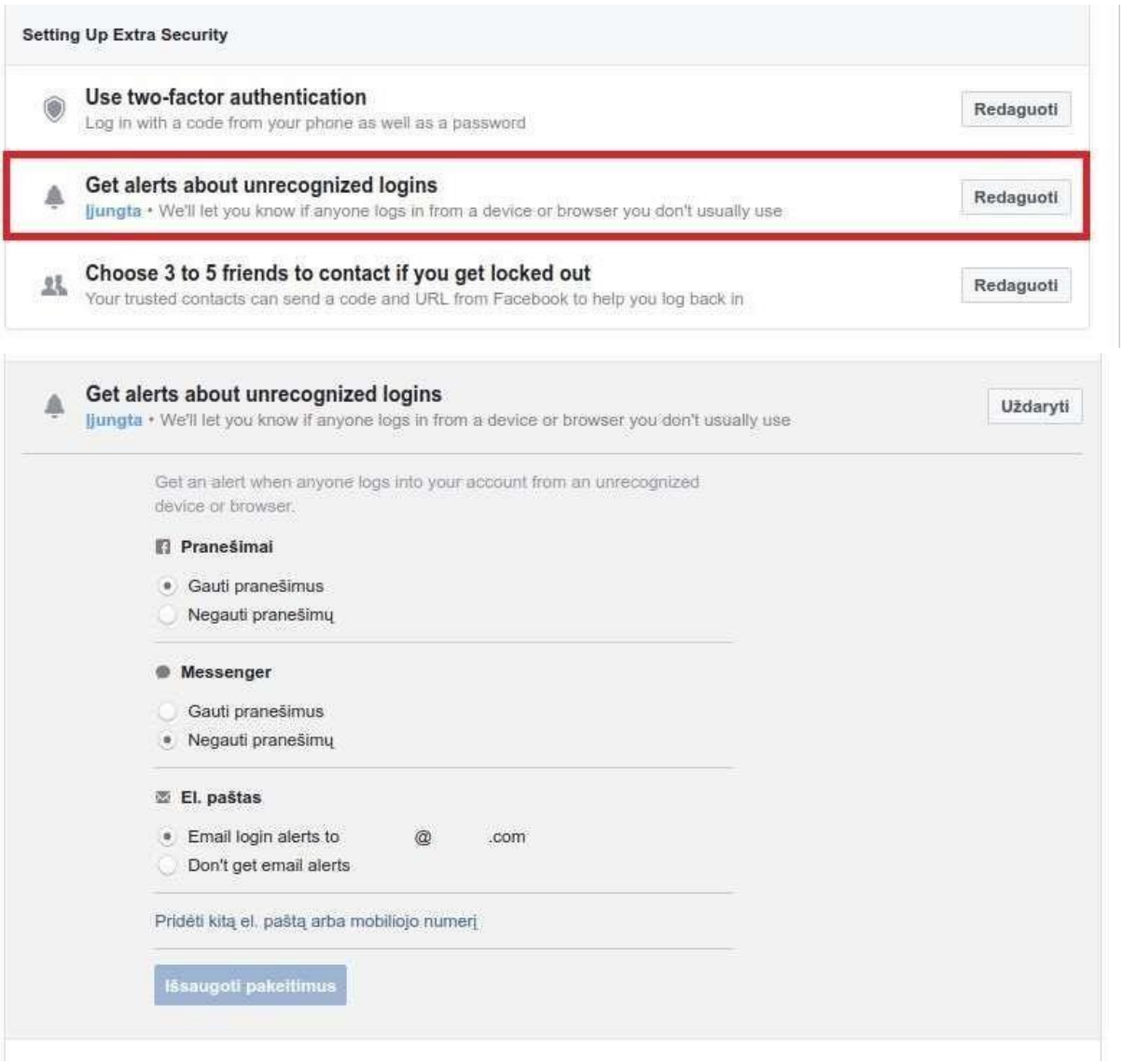
Anbefalinger om, hvordan man forhindrer indbrud

- Brug en sikker adgangskode (det anbefales, at adgangskoden er mindst 9 tegn, inklusive store og små bogstaver, tal og tegnsætning);
- Fortæl ikke din adgangskode til nogen.
- Brug ikke den samme adgangskode, du bruger til andre konti;
- Log ikke på din konto på offentlige enheder;
- Undgå at placere overdreven information på sociale netværk;
- Brug tofaktorautentisering (Indstillinger ➔ Sikkerhed og login)



Figur 2 Konfigurer tofaktorautentisering

- Indstil for at modtage e-mail. Underret dig om mislykkede login til din konto (Indstillinger ➔ Sikkerhed og login).



Figur 3 Underretninger om mislykket login til din konto

Hvad skal jeg gøre, hvis jeg bemærker mistænksom aktivitet eller mister min Facebook-konto? Hvis du har mistanke om, at tredjeparter har adgang til din konto:

- Skift din adgangskode så snart a *s* muligt;
- Kontroller for mistænkelige forbindelser (Indstillinger ➔ Sikkerhed og tilslutninger), skal du afbryde følgende enheder, når du bemærker det:

Figur 4 . De enheder, der er logget ind på din konto

- Hvis du ikke kan logge ind på din konto, kan du prøve at gendanne den ved hjælp af din e-mail;
- Du kan rapportere en mistet konto - https: //www.facebook. dk / hackede
- Hvis du ikke klarer gendanne din konto selv, kan du kontakte retshåndhævelse.

[Nøgleord: facebook, konto, private data, social securit y, meddelelse].

Dette projekt er finansieret med støtte fra Europa-Kommissionen. Denne publicati om [meddelelse] afspejler kun forfatterens synspunkter, og Kommissionen kan ikke holdes

GENERATION DATA

USING DATA FOR PROFIT

Skadelig E mails Casestudie

CYBERNET SIKKERHEDSCENTER UNDER FORSVARINGSMINISTERIET

SENDER TIL E-mailede selskaber i Litauen brev med HARMFUL SOFTWAREKODE

National Cyber Security Center under Ministeriet for National Defense (NKSC) oplyser, at i Litauen spreder e-mails med ondsindet kode. I de seneste dage registrerer NKSC tilfælde af forfalskning af e-mails fra kendte litauiske og udenlandske virksomheder, e-mail-adresser, deres logoer og kontaktoplysninger distribuerer ondsindet softwarekode.

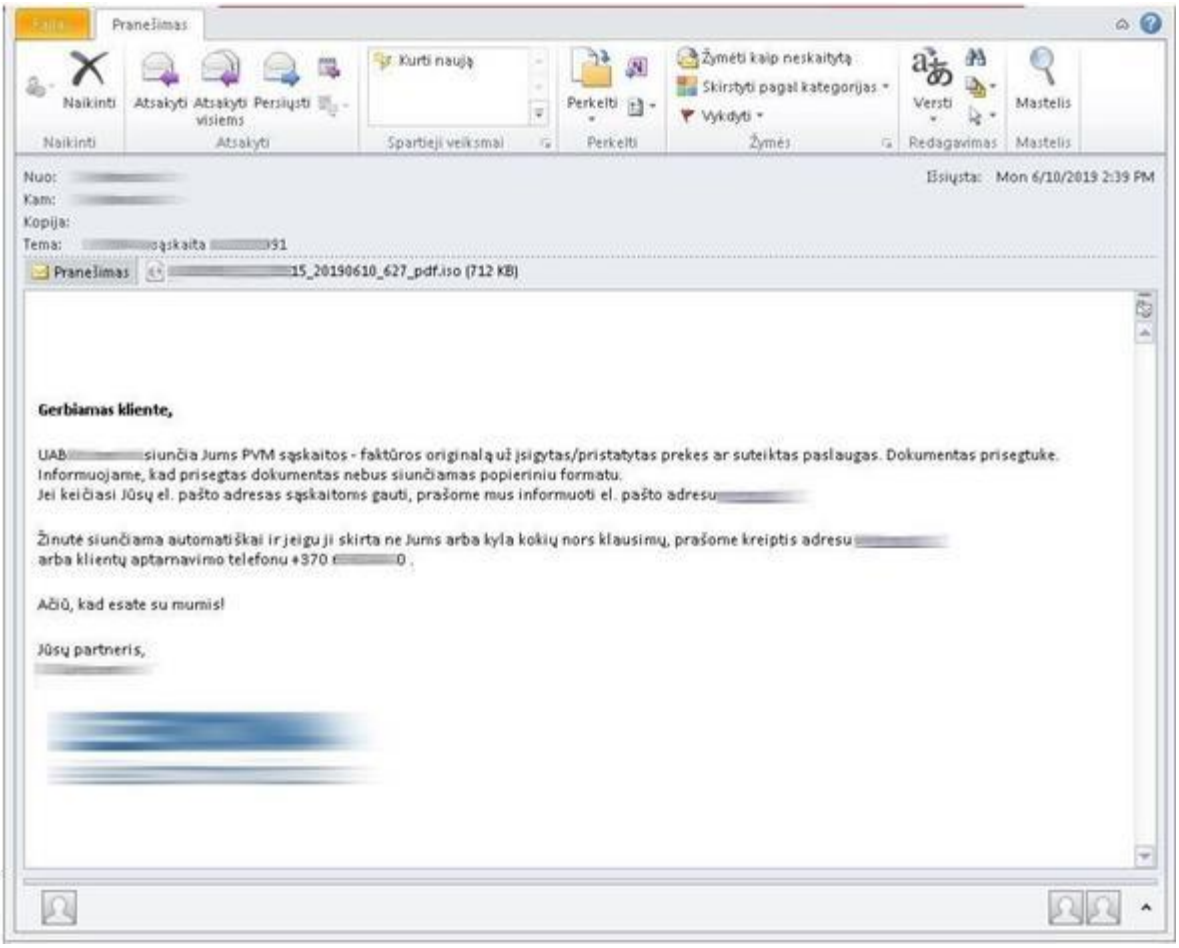


Fig. 1 Falske e-mail et eksempel på et brev, der simulerer en leverandør

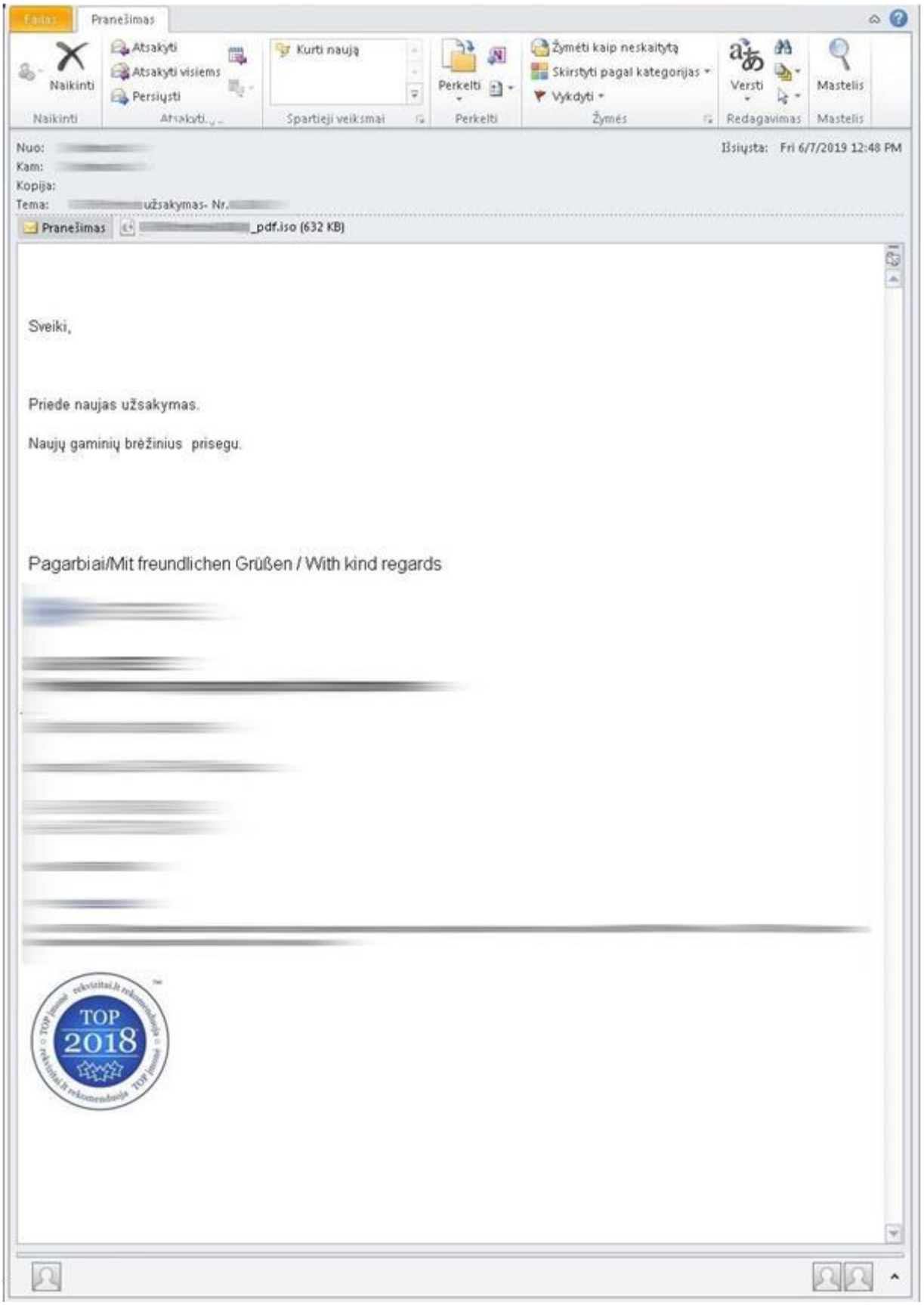

Failas
Pranešimas
Naikinti
Atsakyti
Atsakyti visiems
Persiųsti
Kurti naują
Perkelti
Žymėti kaip neskaitytą
Skirstyti pagal kategorijas
Vykdyti
Versti
Mastelis
Naikinti
Atsakyti...
Spartieji veiksmai
Perkelti
Žymės
Redagavimas
Mastelis
Nuo:
Kam:
Kopija:
Tema: užsakymas- Nr.
Išsiųsta: Fri 6/7/2019 12:48 PM
Pranešimas
_pdf.iso (632 KB)
Sveiki,
Priede naujas užsakymas.
Naujų gaminių brėžinius prisegu.
Pagarbiai/Mit freundlichen Grüßen / With kind regards
TOP
2018

Fig. Falske e-mail et eksempel på et brev, der simulerer en leverandør

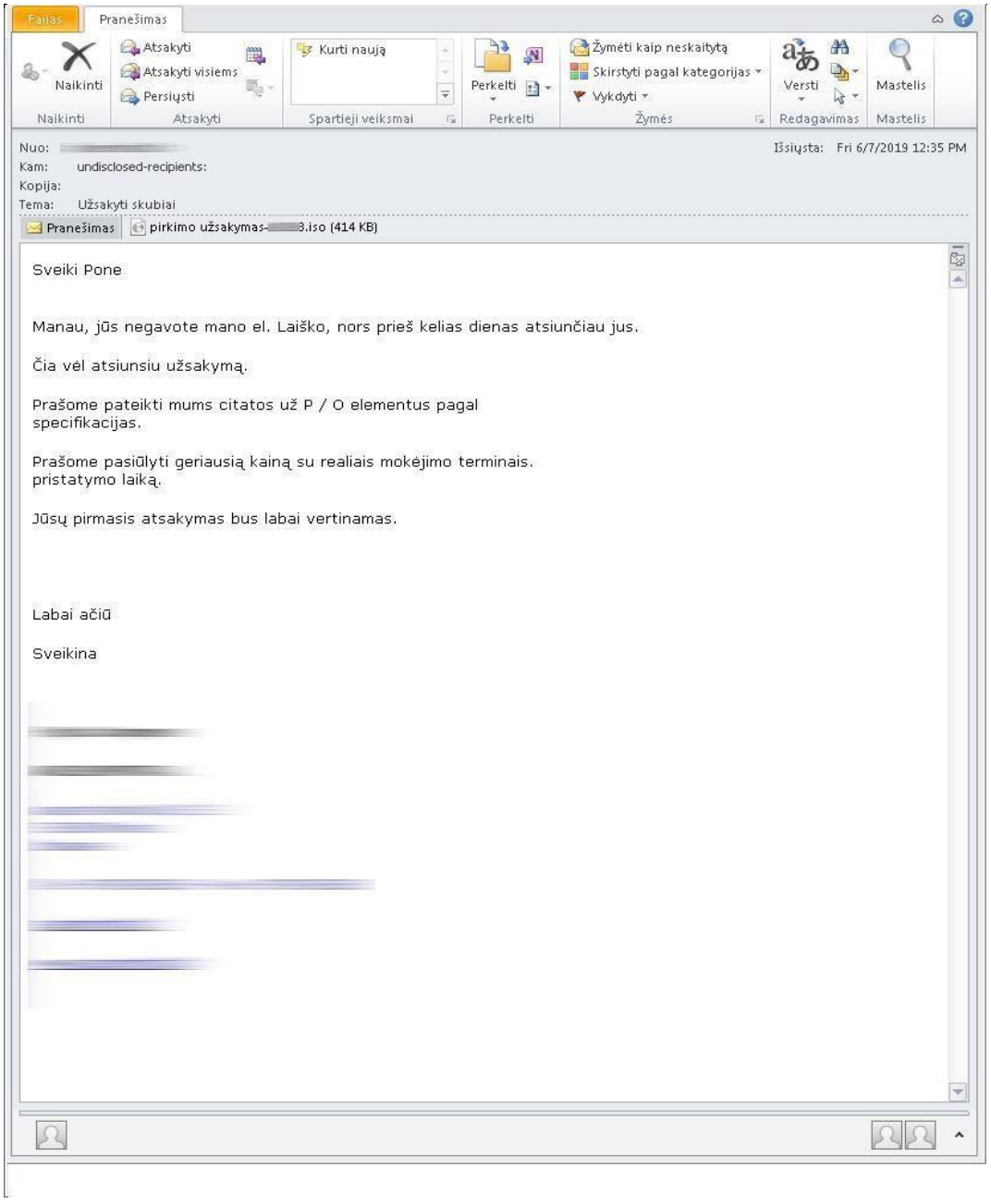


Fig. Falske e-mail et eksempel på et brev, der simulerer en leverandør

Den ondsindede kode er hostet i * .iso-filer, der er knyttet til e-mail. Brev. Den vedhæftede fil indeholder den eksekverbare * .exe-fil. Når vedhæftningen åbnes og eksekverbar * .exe udføres, forsøger ondsindet software at indsamle personlige brugeroplysninger fra computeren, henter computernavnet, forsøger at identificere, om computeren kan få adgang til fjernadgang (eller Remote Desktop-funktionalitet), og sender information til en ekstern server. station og andre efterretningsaktiviteter.

Teksten til brevet er normalt skrevet på litauisk. Beskeden virker realistisk for modtageren, da den sendes fra en kendt og pålidelig adressat, men faktisk er forfalsket.

anbefalinger

Kontroller overskrifterne for meddelelsen for at se, hvem der er den rigtige afsender af meddelelsen (Fra felt). Når man analyserer en header, skal man se på den første modtagne parameter fra bunden. Denne parameter fortæller dig fra hvilken server e-mailen blev sendt. brev. Hvis Fra-feltet er sender@imone.com , skal feltet Modtaget også vise adressedomænet (domæne) "imone.com". I tilfælde af denne fidus viser feltet Modtaget en helt anden data, end hvor meddelelsen blev sendt. Se også: Fig. 4.

Fig. 4 Falske e-mail ægte afsender af meddelelsen

Afhængig af din e-mail-adresse for e-mail-klienter, varierer muligheden for at se overskrifter. Bemærk, at cyberkriminelle også regelmæssigt distribuerer anden ondsindet kode, der udnytter sårbarheder i forskellige software, og vi anbefaler, at du regelmæssigt opdaterer dit antivirus, operativsystem og anden software, du bruger.

For at hjælpe med at forhindre spam anbefaler vi, at du aktiverer og korrekt konfigurerer SPF (Sender Policy Framework) -funktionalitet for at spam e-mail-kontakter. Denne funktion skal bruges med ekstra forsigtighed, da forkerte indstillinger kan medføre, at nogle meddelelser leveres til deres modtagere.

Som en påmindelse er nøglen konstant opmærksom og kritisk over for indgående e-mails.

[Nøgleord: falsk e-mail, ondsindet softwarekode, spam].

Dette projekt er finansieret med støtte fra Europa-Kommissionen. Denne publikation [meddelelse] afspejler kun forfatterens synspunkter, og Kommissionen kan ikke holdes ansvarlig for nogen brug, der måtte blive gjort af de informationer, der er indeholdt deri.