H1 WETGEVING – WAT MAG WEL EN WAT NIET?

1.1 Inleiding

Wat mag wel en wat mag niet? Je zou zeggen dat er overal wetten en regels voor zijn en dat daarmee een behoorlijke mate van duidelijkheid wordt geschapen. Maar hoe zit dat dan bijvoorbeel met het betalen van losgeld om je ‘gegijzelde’ data weer vrij te krijgen? Zijn daar afspraken voor? Is daar wettelijk iets voor geregeld? En kun je bedrijven dwingen om mee te werken hun eigen beveiligingen ‘om zeep’ te helpen? Mag dat?

1.2 Betalen aan criminelen

Je data zijn gegijzeld. Probleem, want er is geen adequate backup. Er blijft blijkbaar niets anders over dan toe te geven aan de eis, dus betalen. Is dit strafbaar?

Een vraag hierover werd gesteld op ‘security.nl’

Opdracht 1.

Lees het onderstaande artikel door en beantwoord de vragen.

Juridische vraag: Is het strafbaar om losgeld te betalen bij ransomware?

woensdag 8 januari 2020, 11:17 door **Arnoud Engelfriet**

Vraag: De geruchten worden steeds sterker dat de Universiteit Maastricht **losgeld betaalde** om haar door Clop gegijzelde systemen terug te krijgen. Nu vroeg ik me af of dat wel mag eigenlijk, losgeld betalen. Moet je niet zoiets via de politie laten lopen?

Antwoord: Ransomware zoals Clop wordt een steeds groter probleem, getuige de vele berichten over ransomware hier op Security.nl alleen al. Het is haast de perfecte misdaad: je ontkomt haast niet aan betalen (tenzij je heel hard je best doet, zie **topdraadje** maar dat lukt vele organisaties niet) en de daders opsporen lukt haast niet. Want waar je een zak geld achtergelaten in de prullenbak in het park nog kunt volgen, is dat met een cryptomunt niet te doen.

Het is niet strafbaar om losgeld te betalen. Dat zou ook wel erg onethisch zijn, slachtoffers van een misdrijf zet je zo klem terwijl ze een geliefde (of heel waardevol object) kwijt zijn en terug kunnen krijgen met dat geld. Dat kun je niet maken als wetgever. Natuurlijk is het beter de politie hierover te laten beslissen, want wellicht weten die een manier om met de betaling de daders op te sporen.

Bij ransomware lees je vaak dat **verzekeraars betalen** wanneer ransomware heeft toegeslagen bij een polishouder. Zakelijk is het immers puur een rekensom: wat kost het om het hele systeem terug te zetten, en hoe hoog is het losgeld? Verrassend genoeg blijken veel ransomware-verspreiders namelijk gewoon de sleutel te geven als je betaalt. Logisch vanuit hun perspectief, want dan gaan de betalende slachtoffers anderen adviseren om ook te betalen. En dit soort misdaad moet het van vele gewillige slachtoffers hebben.

Voor een individueel slachtoffer is het dus niet gek om gewoon te betalen, hoewel maatschappelijk gezien dat natuurlijk buitengewoon onwenselijk is. Voor een verzekeraar voelt het gekker: die heeft meer klanten die mogelijk slachtoffer kunnen worden, en veroorzaakt zo meer claims bij zichzelf (en concullega's). Maar voor het individuele geval zou het ook bij de verzekeraar een prima oplossing kunnen zijn.

Ik ken geen wet die expliciet verbiedt dat een verzekeraar losgeld betaalt. Als de verzekeraar dit in de polis zet als recht, dan zou dat waarschijnlijk in strijd met de openbare orde of goede zeden zijn (art. 3:40 BW). Maar dat levert volgens mij alleen op dat de klant de verzekeraar niet kan dwingen te betalen (een dergelijke verbintenis is immers nietig) of dat de verzekeraar het geld als onverschuldigd betaald kan terugvorderen bij de ransomware-verspreider (en dat heeft geen betekenis). Ik ken geen artikel uit het wetboek van strafrecht dat je tegen zo'n betalende verzekeraar in kunt zetten. Waarschijnlijk is het nooit

verboden omdat niemand er aan gedacht heeft dat dit grootschalig een ding kon worden - bij traditionele gijzelingen is de politie er meestal bij betrokken, en die kan dan bepalen wat wijsheid is.

*Arnoud Engelfriet is Ict-jurist, gespecialiseerd in internetrecht waar hij zich al sinds 1993 mee bezighoudt. Hij werkt als partner bij juridisch adviesbureau **ICTRecht**. Zijn site **Ius mentis** is één van de meest uitgebreide sites van Nederland over internetrecht, techniek en intellectueel eigendom. Hij schreef twee boeken, **De wet op internet** en **Security: Deskundig en praktisch juridisch advies**.*

(Bron: https://www.security.nl/posting/638415/Juridische+vraag%3A+Is+het+strafbaar+om+losgeld+te+betalen+bij+ransomware%3F)

Vragen

Briefgeld heeft nummers en kan worden gevolgd.

1. Hoe zit dat met cryptovaluta? Zijn er mogelijkheden om te traceren waar het terechtkomt en wat er verder mee gebeurt?
2. Geef je mening over het (wettelijk) verbieden van het betalen van losgeld (met cryptovaluta) als duidelijk is dat het gaat om een betaling aan criminelen (zoals bij ransomware).

1.3 Hoezo illegaal?

Programmeren, kan leuk zijn om te doen. Mag je eigenlijk een virus ontwikkelen, zelfs als je het niet gebruikt? En zo ja, wat zijn dan voor mij de grenzen?

Opdracht 2.

Lees het onderstaande artikel door en beantwoord de vragen.

Juridische vraag: Is het maken van software voor een DDoS aanval illegaal?

woensdag 25 september 2019, 10:32 door Arnoud Engelfriet

Vraag: Op het forum las ik de vraag: "Is het maken van software voor een DDoS aanval illegaal?" Kun je daar duidelijkheid over geven?

Antwoord: Het hangt van het beoogde doel van de software af of het illegaal is om deze te maken. De wet stelt namelijk strafbaar het maken, verkopen, verspreiden et cetera van een middel om een ddos aanval te plegen (artikel 139d lid 2 Strafrecht). Het moet dan gaan wel om een "technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf".

In de comments lees ik onder meer dat mensen wijzen op de bekende tool ping(1), waarmee je kunt kijken of een bepaald ip-adres bereikbaar is via internet. Deze beschikt over een flood-optie waarbij heel veel data wordt verstuurd. Daarmee kun je een (d)dos aanval plegen als je de ping richt op je slachtoffer en langdurig met die optie actief pings stuurt. Maar ik kan met de beste wil van de wereld dat geen "hoofdzakelijk geschikt gemaakt of ontworpen" noemen.

Een tool die is voorzien van uitleg hoe je heimelijk deze bij anderen installeert en vervolgens via internet commando's stuurt om vanaf hun computers een dos-aanval uit te voeren, zou ik wel degelijk 'ontworpen' voor dat misdrijf noemen. Het zal dus heel erg neerkomen op hoe de tool wordt gepresenteerd, welke toelichting erbij staat en wat uiteindelijk de algemene indruk is. Ja, dat is vaag maar voor juristen is dat niet erg.

Let op dat het verder niet uitmaakt of je de software verspreidt of voor jezelf houdt. Ook alleen maar zelf maken is in theorie al strafbaar (hoewel de vraag is hoe iemand er dan achter komt dat je het hebt).

*Arnoud Engelfriet is Ict-jurist, gespecialiseerd in internetrecht waar hij zich al sinds 1993 mee bezighoudt. Hij werkt als partner bij juridisch adviesbureau **ICTRecht**. Zijn site **Ius mentis** is één van de meest uitgebreide sites van Nederland over internetrecht, techniek en intellectueel eigendom. Hij schreef twee boeken, **De wet op internet** en **Security: Deskundig en praktisch juridisch advies**.*

(Bron: https://www.security.nl/posting/625465/Juridische+vraag%3A+Is+het+maken+van+software+voor+een+DDoS+aanval+illegaal%3F)

Vragen

3. Zoek het, in het artikel genoemde, wetsartikel op en citeer dit.
4. Leg in eigen woorden uit wat daarmee wordt bedoeld.

1.4 Aansprakelijk of niet?

Je hebt schade geleden door een aanval vanuit een botnet. Dat is toch wel naar. Wie gaat dat betalen? Is er sprake van schuld of van opzet?

Opdracht 3.

Lees het onderstaande artikel door en beantwoord de vragen.

Juridische vraag: Is een IoT-eigenaar aansprakelijk voor schade door een botnet waar zijn apparaat onderdeel van is?

woensdag 21 augustus 2019, 10:39 door Arnoud Engelfriet

Vraag: Stel dat je als partij wordt aangevallen door een botnet dat is geactiveerd vanuit allerlei IoT-systemen. En stel dat ik een aantal van die systemen kan herleiden tot hun Nederlandse eigenaren, laten we zeggen professionele partijen (bedrijven). Kun je dan die eigenaren aansprakelijk stellen voor je schade?

Antwoord: Wanneer je in Nederland schade lijdt door iemands onrechtmatig handelen, dan kun je dat inderdaad verhalen. Het uitvoeren van een denial-of-service aanval (wat ik maar even als invulling van die aanval kies, een computervredebreuk met datavernieling kan natuurlijk ook) is onrechtmatig want strafbaar, dus de dader(s) van zo'n aanval kun je aansprakelijk stellen.

Meestal is het grootste probleem dat je die aanvallers niet kunt achterhalen, maar bij een botnet dat bestaat uit gehackte IoT-apparaten (lees: nalatig slecht ontworpen en geüpdatete kastjes) kan dat inderdaad wel eens anders komen te liggen. Daar wordt nul moeite gedaan de afkomst te verhullen, en als de IP-adressen van die apparaten ook nog eens tot bedrijven te herleiden zijn dan heb je inderdaad vrij snel het adres voor een civielrechtelijke dagvaarding.

Het probleem hier is denk ik lastiger: in hoeverre kun je deze IoT-eigenaren juridisch een verwijt maken? Oftewel hebben zij wel onrechtmatig gehandeld? Zij hebben niet zelf de aanval geïnitieerd of gecoördineerd, dat was de botnet-herder immers. Op eerste gezicht zijn ze dan als willoos werktuig (prachtige juridische term) aan te merken, en daarmee niet aansprakelijk.

Als je de strafwet erbij pakt, dan is er wellicht nog een haakje: artikel 350b Strafrecht verklaart het strafbaar als het jouw schuld is dat een aanval zorgt voor schade (zoals ontoegankelijk zijn van een dienst of gewist worden van gegevens) bij een slachtoffer. Schuld is hier een trapje lager dan opzet (dat staat in 350a), dus kan ook mensen treffen die geen aanval wilden uitvoeren maar dat toch verweten kan worden.

De analyse of sprake is van schuld is juridisch een heel verhaal maar kort door de bocht komt het er voor mij op neer dat ze hun gedrag eigenlijk gewoon hadden moeten aanpassen. Hoe kon je dat nou laten gebeuren, had nou even nagedacht.

Persoonlijk ben ik van mening dat als je als bedrijf zogenaamde smart spullen in gebruik neemt, je moet zorgen voor een goede beveiliging daarvan. Anno 2019 moet iedereen (zakelijk dan) weten dat die apparaten zo lek als een mandje zijn, dus daar moet je dan maatregelen tegen nemen. Doe je dat niet, dan ben je nalatig en wat mij betreft aansprakelijk voor schade. Daar staat tegenover dat je door de leveranciers snel omver geblazen wordt met mooie taal dat die apparaten veilig zijn, en het is vaak gewoon lastig na te gaan óf je apparaten veilig zijn, de laatste firmware hebben et cetera.

Als laatste kanttekening geldt wel dat je als zo'n schuldige alleen aansprakelijk bent voor de schade van jóuw bijdrage, niet voor de gehele schade die al die kastjes samen hebben aangericht. Dat zal bij een gemiddelde aanval nog eens best beperkt zijn, als je überhaupt al een getal kunt plakken op de precieze bijdrage van dat ene kastje van die ene strandtent met gehackte surfweercam of die smart koelkast van die hippe startup.

*Arnoud Engelfriet is Ict-jurist, gespecialiseerd in internetrecht waar hij zich al sinds 1993 mee bezighoudt. Hij werkt als partner bij juridisch adviesbureau **ICTRecht**. Zijn site **Ius mentis** is één van de meest uitgebreide sites van Nederland over internetrecht, techniek en intellectueel eigendom. Hij schreef twee boeken, **De wet op internet** en **Security: Deskundig en praktisch juridisch advies**.*

(Bron: https://www.security.nl/posting/621424/Juridische+vraag%3A+Is+een+IoT-eigenaar+aansprakelijk+voor+schade+door+een+botnet+waar+zijn+apparaat+onderdeel+van+is%3F)

Vragen

5. Zoek het, in het artikel genoemde, wetsartikel op en citeer dit.
6. Leg in eigen woorden uit wat daarmee wordt bedoeld.

1.5 San Bernardino

Bij een aanslag in San Bernardino kwamen op 2 december 2015 veertien mensen om het leven en werden er tweeëntwintig zwaar verwond. Een stel terroristen (een echtpaar) opende het vuur in een overheidsgebouw. Later kwam dit echtpaar om het leven bij een schotenwisseling met de politie.

Opdracht 4.

Lees onderstaande nieuwsartikelen door en beantwoord de vragen.

ARTIKEL 1

Bloedbad San Bernardino: Zeker 14 doden

02 december 2015 22:58

Aangepast: 03 december 2015 00:40

Beeld © EPA

Bij de schietpartij in de Amerikaanse stad San Bernardino zijn zeker 14 doden gevallen. Ook zijn er 17 gewonden gevallen. Dat heeft de politie zojuist bekendgemaakt tijdens een persconferentie.

De eerste melding van de schietpartij bij het Inland Regional Center kwam rond 20:00 uur Nederlandse tijd. Drie daders zijn het gebouw ingegaan. Bij binnenkomst zijn ze gaan schieten. Er waren op tot moment honderden mensen in het gebouw. De schietpartij heeft volgens de politie enkele minuten geduurd.

Vrije voeten

"Ze waren voorbereid om te doen wat ze deden, alsof ze op een missie waren", zei de politiechef over de schutters. Ze zijn nog op vrije voeten. De politie meldt dat het op dit moment niet duidelijk is waar de schutters zijn. De explosievenopruimingsdienst onderzoekt het gebouw nog. Er zouden verdachte pakketten gevonden zijn.

Over het motief van de schutters is nog niets bekend. De politie heeft nog geen aanwijzingen dat het om een terroristische aanslag gaat.

(Bron: https://www.rtlnieuws.nl/buitenland/artikel/833361/bloedbad-san-bernardino-zeker-14-doden)

Vervolg

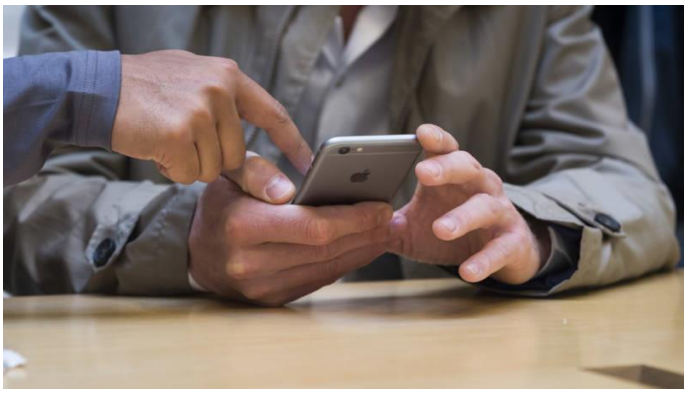
Van een van de schutters werd een iPhone gevonden en dit resulteerde in een rechtszaak. De FBI wilde dat Apple deze telefoon ontsleutelde, maar Apple weigerde hieraan mee te werken. Waarom zou je namelijk de beveiliging van je eigen apparatuur en/of software op het spel zetten? Apple kreeg een rechtszaak aan zijn broek, want ze werden aangeklaagd door de FBI. De rechtszaak liep met een sisser af, omdat er uiteindelijk een andere manier gevonden werd om in de telefoon van de terrorist te komen.

ARTIKEL 2

NOS NIEUWS • ECONOMIE •TECH • 14-06-2018, 09:06 • AANGEPAST 14-06-2018, 10:55

Bekende hackmethode voor iPhones straks vrijwel onbruikbaar

Apple gaat het onmogelijk maken om via een bekende methode iPhones te hacken. Op dit moment kan bijvoorbeeld de politie via de oplaadingang van het toestel met speciale software proberen toegang te krijgen tot de telefoon.



Amerikaanse media schrijven dat Apple een software-update heeft gepland die dit onmogelijk maakt. De wijziging zorgt ervoor dat de telefoon een uur nadat deze voor het laatst ontgrendeld is, digitaal op slot gaat. Dit kan overigens gevolgen hebben voor andere apparaten die gebruik maken van de ingang, bijvoorbeeld om muziek te luisteren. Welke impact dit precies zal hebben is nog onduidelijk.

Ontgrendelcode

Het toestel kan dan nog wel worden opgeladen, maar het is niet meer mogelijk om data te versturen. Daarvoor is de ontgrendelcode nodig. Opsporingsdiensten konden nu via de ingang met speciale software tot maanden nadat de telefoon gevonden is proberen het toestel te '*brute forcen'.* Dit betekent dat een oneindig aantal inlogpogingen wordt gedaan totdat de juiste code is ingevoerd.

Opsporingsdiensten kunnen dergelijke hacksoftware kopen bij gespecialiseerde bedrijven, zoals het Israëlische Cellebrite en het Amerikaanse Grayshift. Beide bedrijven zeggen in staat te zijn zelfs Apples meest recente toestellen, de iPhone X, te kunnen kraken.

De vraag of opsporingsdiensten toegang moeten krijgen tot telefoons leidt al jaren tot spanningen. Deze maatregel van Apple wordt dan ook met boosheid ontvangen, schrijft The New York Times. De krant laat onder meer een chef van een politie-eenheid in de staat Indiana aan het woord, die het hacken van iPhones nodig heeft voor onderzoek naar zaken omtrent internetcriminaliteit tegen kinderen. De eenheid heeft dit jaar 96 iPhones gekraakt met speciale software die het voor 15.000 dollar kocht.

Garantie valt weg

"Dit betekent dat de garantie wegvalt dat je de telefoon binnen een x aantal dagen gekraakt hebt", zegt beveiligingsonderzoeker Rickey Gevers. "Deze methode maakte het mogelijk om iPhones die up-to-date zijn, te kraken. Nu moeten partijen op zoek gaan naar lekken die nog niet zijn gedicht. Dat kan soms maanden duren."

"We hebben groot respect voor opsporingsdiensten", zegt een woordvoerder van Apple tegen Amerikaanse media. "We ontwerpen onze beveiliging niet om hun werk te frustreren." Het is vooralsnog onduidelijk in welke software-update de nieuwe functie, die Apple *USB Restricted Mode* noemt, beschikbaar komt. Een logisch moment zou de lancering van iOS 12 zijn dit najaar, maar Apple wil dat niet bevestigen.

Voor zover bekend heeft de FBI, die de afgelopen jaren flinke kritiek had op Apples beveiligingsbeleid, nog niet gereageerd op het nieuws.

(Bron: https://nos.nl/artikel/2236425-bekende-hackmethode-voor-iphones-straks-vrijwel-onbruikbaar.html)

Vragen

7. Om welk type iPhone ging het?
8. Welk bedrijf heeft de FBI geholpen?
9. Op welke manier?

1.6 Opnieuw ‘gedoe’ met de iPhone

Het wel of niet kraken van de beveiliging van de iPhone blijft de gemoederen bezig houden.

Opdracht 5.

Lees het onderstaande nieuwsartikel – uit het Nederlands Dagblad - zorgvuldig door en beantwoord de vragen.

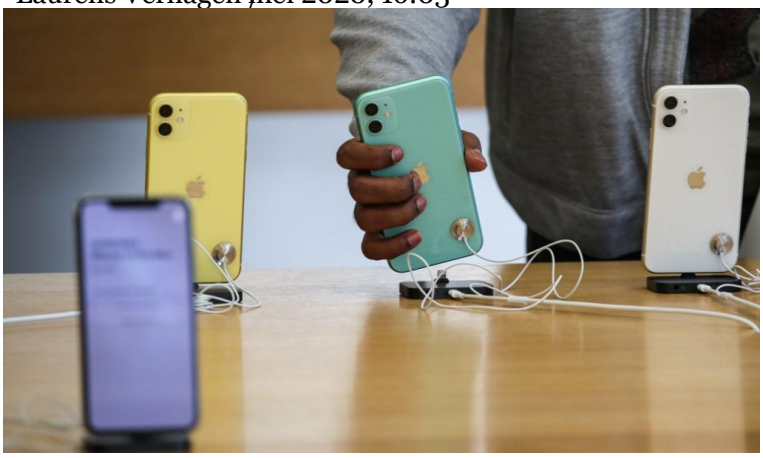
FBI kraakt iPhone en is woedend op Apple

Het is de FBI gelukt om de vergrendelde iPhones open te breken van de man die drie Amerikaanse militairen doodschoot. De FBI wilde dit doen om bewijs te verzamelen, maar fabrikant Apple weigerde hierbij hulp.

Beeld © EPA

Washington DC

Laurens Verhagen / mei 2020, 16:03



Mohammed Saeed Alshamrani schoot een half jaar geleden op een luchtmachtbasis in Florida drie Amerikaanse militairen dood. Al snel rees het vermoeden dat hieraan terroristische motieven ten grondslag lagen. Om hier zeker van te zijn, wilde de FBI toegang tot de iPhones van de aanslagpleger.

Probleem: iPhones zijn bijzonder lastig te ontgrendelen zonder de hulp van de rechtmatige eigenaar. Dat geldt zowel voor het openen met vingerafdruk als voor het openen via gezichtsherkenning. Het standpunt van Apple is al jarenlang hetzelfde: we kunnen en willen niet helpen telefoons te ontgrendelen.

Apple zelf kan ook geen toegang krijgen tot de telefoons van zijn klanten. De biometrische informatie van een gezicht of vingerafdruk staat niet op een server bij Apple opgeslagen, maar alleen lokaal op het toestel zelf: een privacyvriendelijkere omgang met de data.

achterdeurtjes

Het alternatief is het inbouwen van achterdeurtjes, maar daarover is Apple duidelijk. ‘Dit zou alleen de goedbedoelende en gezagsgetrouwe burgers schaden die op bedrijven als Apple vertrouwen om hun gegevens te beschermen’, zei topman Tim Cook bijvoorbeeld al in 2016, toen een vergelijkbare zaak speelde.

Het probleem is namelijk dat het bewust inbouwen van achterdeurtjes voor bijvoorbeeld de FBI onherroepelijk betekent dat de toestellen ook voor andere, buitenlandse diensten of voor criminelen een makkelijker doelwit zijn.

De FBI heeft dus, net als in 2016, zelf het toestel van de schutter geprobeerd te openen. Dat was niet eenvoudig, blijkt uit de gezamenlijke verklaring van Justitie en de federale inlichtingendienst. ‘Met dank aan het geweldige werk van de FBI – en zonder dank aan Apple – waren we in staat om Alshamrani’s telefoons te ontgrendelen’, aldus minister van Justitie William Barr. De minister wees er ook nog fijntjes op dat het gedoe niet alleen kostbare tijd heeft gekost, maar de Amerikaanse belastingbetaler ook veel geld.

zwakkere beveiliging

Zowel Justitie als de FBI grijpen de Alshamrani-zaak aan om opnieuw te pleiten voor zwakkere beveiliging en minder encryptie op telefoons. De houding van Apple is in de ogen van Barr ‘onacceptabel’. Apple zelf denkt daar uiteraard anders over. Het bedrijf is bereid inlichtingendiensten te helpen, maar niet tegen iedere prijs. Zo werd eerder dit jaar bekend dat Apple onder druk van Justitie zijn plan liet varen om backups in zijn clouddiensten te versleutelen.

Bezitters van iPhones of andere Apple-apparatuur kunnen ervoor kiezen alles wat op die apparaten staat ook op de servers van Apple te zetten. Zo’n reservekopie is praktisch bij bijvoorbeeld overstappen op een nieuw apparaat of bij verlies van een toestel, maar biedt dus minder privacy en zekerheid. Deze cloud-omweg bood in het geval van Alshamari echter geen soelaas: niet alle informatie op zijn telefoon stond ook opgeslagen in de cloud.

In een verklaring tegenover The Verge benadrukt Apple dat het de FBI zo goed mogelijk heeft geholpen. Maar, zegt het bedrijf ook: klanten over de hele wereld moeten erop kunnen vertrouwen dat hun informatie veilig is.

spionagesoftware

Of dat altijd het geval is, is overigens niet zeker. NBC News schrijft namelijk op basis van bronnen dat de Amerikaanse politie in staat is om de toegangscode van een iPhone te registreren op het moment dat gebruikers deze invoeren. Hiervoor is het dan wel nodig dat er spionagesoftware op de iPhone is geïnstalleerd. Deze spyware is volgens de nieuwszender ontwikkeld door Grayshift, een Amerikaans bedrijf dat hierin gespecialiseerd is. De methode werkt niet voor het gebruik van vingerafdruk of gezichtsherkenning.

(Bron: Nederlands Dagblad – 20 mei 2020 - FBI kraakt iPhone en is woedend op Apple)

Vragen

Bij onderstaande opdrachten mag je gebruik maken van Nederlandse wetgeving, maar ook van Amerikaanse wetgeving.

10. Geef een duidelijk argument en onderbouw dit met bronnen vóór het standpunt van Apple.
11. Geef een duidelijk argument en onderbouw dit met bronnen tégen het standpunt van Apple.
12. Wat is je eigen mening hierover?

Opdracht 6.

Zoek artikel 138ab op van het Wetboek van Strafrecht en lees dit artikel zorgvuldig door en beantwoord de vragen.

De FBI, een overheidsinstantie dus, heeft zich laten bijstaan door een bedrijf om de beveiliging van de genoemde iPhone te kraken.

Vragen

13. Geeft het bovennoegmde wetsartikel in eigen woorden weer.
14. De overheid is er ten dienste van de burgers. Vind je, dat op grond van het **bovengenoemde wetsartikel** overheidsfunctionarissen in Nederland wél of niet beveiligingen mogen kraken? Motiveer je antwoord.

Opdracht 7.

Zoek de laatste versie op van de Wet op de inlichtingen- en veiligheidsdiensten (de zogenaamde ‘sleepwet’) en beantwoord de vragen.

Vragen

15. Welke ‘versie’ is dit?

‘Blader’ deze wet door, lees de titels van de hoofdstukken en probeer je een beeld te vormen van de inhoud.

16. Biedt, volgens jou, deze wet mogelijkheden/bevoegdheden voor overheidsdiensten om in te kunnen grijpen door het (laten) kraken van een beveiliging? Zo ja, in welk hoofdstuk denk je dat te vinden en aan welk artikel ontleen je je mening? Zo niet, wat is dan de bedoeling van deze wet?
17. Vanaf 1 maart 2019 heeft de Nederlands politie verregaande bevoegdheden met betrekking tot het verkrijgen van data gekregen. Welke bevoegdheden zijn dat en hoe heet de wet waarin dat is geregeld?

Opdracht 8.

Zoek artikel 8 van het Europees Verdrag voor de Rechten van de Mens op, lees dit zorgvuldig door en beantwoord de vraag.

Vragen

18. Leg in eigen woorden uit wat daarmee wordt bedoeld.

1.7 Aansprakelijk of niet?

Je bent ICT-expert, maar je klant luistert niet goed naar jouw adviezen en wordt vervolgens gehackt. Ben jij aansprakelijk?

Opdracht 9.

Lees het onderstaande artikel door en beantwoord de vragen.

Maakt onverstandig handelen op verzoek van de klant een IT-dienstverlener schadeplichtig?

woensdag 10 juni 2020, 11:18 door Arnoud Engelfriet

Juridische vraag: Ik werk als IT-automatiseerder voor mkb'ers. Een klant wil volledig opnieuw geautomatiseerd worden, dus ik ben druk bezig met netwerk, software, firewalls et cetera. Alleen vindt de klant mijn gekozen firewall- en VPN-oplossing te duur, zijn de wachtwoorden te moeilijk (het liefst heeft hij drieletterige wachtwoorden geloof ik) en wordt mijn advies over backups genegeerd. Ben ik nu aansprakelijk als ik toegeef?

Antwoord: Ja, dat is heel goed mogelijk. Je hebt écht een zorgplicht en dat betekent ook doorvragen en vasthoudend doen als de klant er niet aan wil. Doe je dat niet, en gaat er wat mis, dan hang jij voor de kosten die het bedrijf heeft geleden. Je komt niet weg met “ik heb het voorgesteld maar ze vonden het te duur / ze wilden er niet aan”. Onverstandig handelen op verzoek van de klant maakt je schadeplichtig. En nee, je algemene voorwaarden gaan je niet redden.

Een recent gepubliceerd vonnis uit 2018 laat goed zien hoe de rechter hiermee omgaat. Een IT-dienstverlener en automatiseerder had aan een administratiekantoor aangeboden om de IT-infrastructuur opnieuw in te richten. Er werd een nieuw netwerk aangelegd en allerlei onderhoud uitgevoerd. Wat me daarbij opvalt, is dat er geen uitgebreide afspraken gemaakt maar op basis van goed vertrouwen tegen een vast tarief (380 euro per maand, ja maand) werd gewerkt.

In 2017 werd het kantoor slachtoffer van ransomware. Zij heeft ervoor gekozen te betalen en zo haar bestanden terug te krijgen, kennelijk de enige manier want er was iets met de back-ups en daar kom ik zo op. Een cybersecuritybedrijf kwam tot de bevinding dat er een backoffice-account was met een zwak wachtwoord én dat poort 443 open stond zodat je vanaf internet een remote desktop kon starten. In juridische taal: slordigheden.

Ook signaleerde het securitybedrijf dat er geen maatregelen omtrent wachtwoorden waren genomen, dat er niet met VPNs werd gewerkt én er dus geen fatsoenlijke back-upvoorziening was. Met name dat laatste: "[Deze aanval] had voorkomen kunnen worden met een op de juiste manier ingeregelde backup."

Wat was nu het probleem daarmee? Nou ja, er was bij het offertetraject gesproken over een "totaalpakket" aan IT-dienstverlening. Het kantoor stelde nu dat beveiliging daar natuurlijk ook bij hoort, wat in 2017 best wel redelijk was als uitgangspunt. En aangezien die duidelijk was verzaakt, moest het IT-bedrijf de kosten van herstel (de bitcoins) en bereddering (de factuur van het securitybedrijf) komen vergoeden.

Maar het IT-bedrijf wierp daartegen op dat de klant steeds al zijn voorstellen op dat gebied had afgewezen. Zo vond men een firewall te duur, en waren alle back-upoplossingen te ingewikkeld – inclusief de oplossing van een externe USB-schijf die je dan in het weekend mee naar huis nam. Ook had het personeel kennelijk moeite met stevige wachtwoorden, zodat in arren moede dan maar simpele wachtwoorden werden toegestaan.

Je hebt dus een zorgplicht als IT-leverancier (art. 7:401 BW). Dat wil zeggen dat je moet handelen zoals een ‘goed’ vakgenoot zou doen. Dat is een open norm, en het hangt dus volledig af van de situatie wat dat precies inhoudt. Maar wat het niet inhoudt, is dat als de klant zegt "eh firewall is te duur en wachtwoorden graag alleen letters" dat je dan zegt "oké gaan we doen, wat jij wil". Het is en blijft jouw

verantwoordelijkheid dat er een fatsoenlijke oplossing komt. Kan dat niet, dan moet je de opdracht teruggeven.

Iets specifieker, als de klant je opdraagt het op een ongepaste of onveilige manier te doen, dan zegt art. 7:402 BW:

De opdrachtnemer die op redelijke grond niet bereid is de opdracht volgens de hem gegeven aanwijzingen uit te voeren, kan, zo de opdrachtgever hem niettemin aan die aanwijzingen houdt, de overeenkomst opzeggen wegens gewichtige redenen.

Natuurlijk, klanten kunnen onverstandig en koppig zijn (zowel alle juristen als alle IT-ers glimlachen nu van herkenbaarheid) maar aangezien jij de professional op dit gebied bent, moet jij die klant bij z'n nekvel pakken en zeggen, zo kan het niet wat u wil. We kunnen het zus doen of zo. Je zet dan bijvoorbeeld alle desktop-firewalls dicht of configureert de router zodat er niet op afstand gewerkt kan worden. Wil men dat toch, ja dan is dat meerwerk want dat moet wel veilig.

Zoals de rechter het formuleert:

Gelet op de afspraak dat hij een totaalpakket inclusief beveiliging zou leveren, in combinatie met zijn professionele deskundigheid, kon hij niet volstaan met een enkele waarschuwing en berusten in de keuzes van O'Cliance.

Dit wil natuurlijk niet zeggen dat je tot in lengte van dagen moet blijven ploeteren tegen de wens van de klant in, zonder extra kosten te mogen rekenen omdat je nu eenmaal een vast maandtarief had afgerekend. Je kúnt op zeker punt best zeggen, goed, dit is het en vanaf hier is het jouw risico. Maar dat kan pas als je uitgebreid hebt voorgelicht en gewaarschuwd, wat niet hetzelfde is als "dit lijkt me niet veilig maar oké". En ook niet als "artikel 14.3 van mijn algemene voorwaarden zegt dat de gevolgen van klantkeuzes voor zijn rekening komen", zoals sommige IT-ers nog wel lijken te denken.

Op één punt had de IT-er het wel goed gedaan en dat waren die zwakke wachtwoorden. Hij had eerst keurig ingewikkelde wachtwoorden ingesteld, maar de klant had daar moeilijk over gedaan. En pas na diverse rondes discussie én een uitdrukkelijke waarschuwing gaf hij zich gewonnen:

Met betrekking tot deze wachtwoorden staat bovendien vast dat [gedaagde] aanvankelijk complexe wachtwoorden had ingesteld, maar dat hij deze op uitdrukkelijk verzoek van [het administratiekantoor] heeft vereenvoudigd. Op de zitting heeft [betrokkene] hierover verklaard dat hij herhaaldelijk met [gedaagde] over de wachtwoorden heeft gesproken en dat hij zich ervan bewust was dat het gebruik van simpele wachtwoorden risico's met zich bracht.

Daarom komt een derde van de schade voor eigen risico van de klant. En die schade? Ja, een slordige 15 duizend euro: gederfde omzet door bedrijfsstilstand, de kosten van het onderzoek én de drie bitcoins die nodig waren om de data terug te krijgen. Wellicht dat algemene voorwaarden deze vordering iets hadden kunnen dempen, maar schending van je zorgplicht is een vrij fundamenteel ding dus denk niet dat je wegkomt met enkel dat zinnetje "gederfde omzet komt niet voor vergoeding in aanmerking" of iets dergelijks.

De belangrijkste les voor mij: zorg dat je blijft communiceren met je klant en dat je daarin de risico's ook écht duidelijk maakt. In taal die de klant snapt, met waarschuwingen die er niet om liegen en blijf aandringen op een bevestiging van de vorm "ik snap de risico's en ik wil het tóch zo". Dat doe je in de conversatie, niet verstopt in je voorwaarden en niet met een bulletpoint in je offerte. En die conversatie die log je en je komt erop terug als de situatie rijp lijkt voor verbetering. Dat is hoe een goed IT-er zorgt voor zijn klanten.

*Arnoud Engelfriet is Ict-jurist, gespecialiseerd in internetrecht waar hij zich al sinds 1993 mee bezighoudt. Hij werkt als partner bij juridisch adviesbureau **ICTRecht**. Zijn site **Ius mentis** is één van de meest uitgebreide sites van Nederland over internetrecht, techniek en intellectueel eigendom. Hij schreef twee boeken, **De wet op internet** en **Security: Deskundig en praktisch juridisch advies**.*

(Bron: https://www.security.nl/posting/660492/Maakt+onverstandig+handelen+op+verzoek+van+de+klant+een+IT-dienstverlener+schadeplichtig%3F)

Vragen

19. Zoek het genoemde vonnis op en neem het globaal door. https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2018:10124
20. Wat is reconventie?
21. De 'gedaagde' wordt veroordeeld om aan O'Cliance een bedrag van € 10.271,93 te betalen. Leg uit hoe dit bedrag tot stand is gekomen.
22. Geef een korte, heldere samenvatting met daarin
    a. de aanleiding tot het geschil
    b. de rol van True-xs
    c. de vorderingen van beide partijen
    d. de uitspraak van de rechter
    e. de les hiervan voor zowel de klant, als voor het IT-bedrijf

Opdracht 10. (alleen of met z'n tweeën)

Woningen kunnen gesloten worden, een straatverbod kan worden opgelegd. Zoek uit waarom het opleggen van een internetverbod, bijvoorbeeld omdat iemand online criminele activiteiten heeft ondernomen, niet zo gemakkelijk is als het misschien lijkt. Of kan het toch wel? Geef goede argumenten en gebruik hierbij wetgeving, eventuele jurisprudentie, onderzoeken, nieuwsartikelen e.d. Schrijf een reflectie hierover van minimaal 300 woorden of van minimaal 500 woorden als je dit met z'n tweeën doet.

Beoordeling

1 t/m 3	4 t/m 5	6 t/m 7	8 t/m 10
Nauwelijks argumentatie. Veel lijkt kritiekloos overgenomen of nageschreven te zijn. Bronvermelding onvoldoende.	Er worden onvoldoende en/of niet correcte argumenten aangedragen om de mening te onderbouwen. Er worden te weinig bronnen vermeld of bronnen die niet geschikt zijn.	Argumentatie is helder en voldoende overtuigend. Verwijzing naar enkele passende bronnen, die op een correcte wijze vermeld zijn. Niet altijd even kritisch.	Uitstekende analyse. Overtuigende argumenten, ook voldoende kritisch, als dat nodig is. Onderbouwd met verwijzingen naar adequate bronnen. Vermeld volgens APA-normen.