www.jusletter-it.eu

Sikander von Bhicknapahari

Cyber-Lösegeldzahlungen

DDoS- oder Virenattacken können mit Lösegeldforderungen einhergehen. Wie ist buchhalterisch damit umzugehen?

Die University of Calgary zahlte CAD 20'000 Lösegeld in Form von Bitcoins, um wieder Zugriff auf ihre Mails zu erhalten. Auch ein Medical Center und sogar ein Police Department in Massachusetts sollen Lösegeld bezahlt haben. Uber bezahlte USD 100'000 an einen Hacker, der Daten von 57 Millionen Gästen und Fahrern gestohlen hatte.

Category: Articles
Region: Switzerland
Field of Law: Informatikrecht; Cybercrime; Gesellschaftsrecht

Citation: Sikander von Bhicknapahari, Cyber-Lösegeldzahlungen, in: Jusletter IT 26 September 2018

Inhaltsübersicht

1. Technische Erläuterungen

[Rz 1] Bei einer DDoS-Attacke wird eine Website innert kürzester Zeit tausendfach aufgerufen mit dem Ziel, dass das System wegen der Datenlast zusammenbricht. Für einen Webshop ein Umsatz-, und damit einhergehend auch ein Kundenverlust, daneben zusätzlich auch ein Reputationsrisiko. Mit einer Viren-Attacke können Programme auf ein Computersystem eingeschleust werden, welche die Daten verschlüsseln. Der Computeranwender kann das System nicht mehr benutzen.[1] Nach Zahlung eines Lösegeldes ist das Computersystem wieder benutzbar.[2]

[Rz 2] Neben dem Lahmlegen eines Systems ist es auch ein Zugriff von unberechtigten Dritten auf ein System möglich. Via bekannten technischen Schwachstellen oder bekannten Benutzernamen mit Passwort dazu, können Daten auf einem System in falsche Hände geraten. Ein solcher «Hack» dient der Datenbeschaffung, z. B. Kreditkartendaten von Kunden.

2. Wie verbuchen?

[Rz 3] Gemäss einer Studie sollen 23% der Schweizer Unternehmen bereit sein, im Falle einer Ransomware-Attacke Lösegeld zu bezahlen, weltweit liegt dieser Wert bei 33%.[3] Bei dieser hohen Quote von Zahlungsbereitschaft stellt sich buchhalterisch die Frage, wie ein solcher Fall erfasst werden soll. Der Geldempfänger ist nicht bekannt und der genaue Geldfluss zum Empfänger nicht nachvollziehbar. Es liegen abgesehen von Printscreens keine Belege vor, allenfalls Mails mit nicht nachvollziehbarem Absender. Solche Belege sind aus handelsrechtlicher Sicht nicht ordnungsgemäss. Ein Beleg soll «Beweis leisten für die gebuchten Vorgänge».[4] Da hier kein Originalbeleg von einem identifizierbaren Dritten vorliegt, und auch die Zahlung keinen Rückschluss

1 Vgl. «Melde- und Analysestelle Informationssicherung MELANI» vom 20. Mai 2015, «DDoS Angriffe und Erpressung: eine äusserst aktuelle Kombination», (https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/ddos_angriffe_und_erpressung.html) und Kurt Sagatz, «Der Tagesspiegel» vom 13. Mai 2017, «Wie Hacker mit Cyber-Attacken Millionen erpressen» (https://www.tagesspiegel.de/weltspiegel/ransomware-wanna-cry-wie-hacker-mit-cyber-attacken-millionen-erpressen/19797626.html) (alle Websites zuletzt besucht am 10. September 2018).

2 Vgl. «BBC» vom 8. Juni 2016, «University pays $20,000 to ransomware hackers» (https://www.bbc.com/news/technology-36478650).

3 Vgl. Ulrike Garlet, «CRN» vom 20. Juni 2018, «Unternehmen geben weniger für IT-Sicherheit aus» (https://www.crn.de/security/artikel-117406.html).

4 Karl Käfer, in: Kommentar zum schweizerischen Privatrecht, Band VIII, 2. Abteilung, Bern 2001, Art. 957 N 146.

auf den Empfänger zulässt, liegt kein solcher Beweis vor.[5] Der vom Gesetz verlangte Nachvollzug eines Sachverhalts lässt sich nicht belegen.[6]

[Rz 4] Auf welchem Aufwandkonto soll eine solche Zahlung erfasst werden, wo in der Rechnungslegung soll wie darüber berichtet werden? Kann ein solcher Fall im übrigen Betriebs- oder Verwaltungsaufwand[7] erfasst werden und unerkannt versickern? Oder wäre dies ein Thema, welches in der Erfolgsrechnung unter «einmalig» oder «ausserordentlich» aufzuführen ist?[8] Letzteres trifft wohl eher zu, denn Lösegeldzahlungen gehören nicht zum üblichen Geschäftsaufwand. Das Lösegeld als Betriebsaufwand zu erfassen wäre zudem ein Hinweis auf eine mangelhafte IT-Sicherheit, als deren Folge man einen solchen Aufwand in Kauf nimmt. Bei Verbuchung und Ausweis unter «einmalig» oder «ausserordentlich» wird ein Kommentar dazu im Anhang notwendig.[9] Die Erfahrung zeigt, dass Auswirkungen einer mangelhaften IT-Sicherheit nicht nur die eigene Firma schädigen kann. Es können auch Kunden und Lieferanten betroffen sein, sei es dass die weltgrösste Reederei keine Aufträge mehr entgegennehmen konnte, seien es Paketkunden, deren Paket nicht verzollt werden konnten.[10] Die Lösegeldzahlung selbst kann im Verhältnis zum Umsatz einen unwesentlichen Betrag darstellen, weshalb auf den ersten Blick kein Kommentar im Anhang notwendig erscheint.[11] Das Schadenspotential einer mangelhaften IT-Organisation ist jedoch wesentlich, deshalb ist eine Kommentierung im Anhang angebracht. Die Aktionäre wissen somit über dieses Missgeschick Bescheid. Sie können sich Gedanken über mögliche finanzielle Auswirkungen solcher Organisationsmängel machen, und auch über die mögliche Verantwortlichkeit der Organe diskutieren.[12]

3. DBG-anerkannter Aufwand?

[Rz 5] Die ESTV teilte auf Anfrage mit, dass zur steuerlichen Abzugsfähigkeit einer solchen Lösegeldzahlung noch keine Erfahrungswerte vorliegen. Die geltende Steuerpraxis liesse jedoch effektiv bezahlte Schmiergelder oder verdeckte Kommissionen trotz ihres widerrechtlichen oder unsittlichen Charakters als Gewinnungskosten bzw. geschäftsmässig begründete Aufwendungen zu. Anzunehmen ist, dass sich die ESTV auf die Rechtsprechung im Zusammenhang mit unsittlichen Einnahmen abstützen wird.[13] Wichtig aus Sicht der ESTV ist jedoch die geschäftsmässige Begründetheit und der Nachweis der Ausrichtung. Mit einem Beleg, der keinen Rückschluss auf den Empfänger des Geldes zulässt, könnte diese Anforderung nicht erfüllt sein.

---

5 Siehe auch Sikander von Bhicknapahari, in: veb.ch Praxiskommentar, 1. Aufl., Zürich 2014, Art. 957a N 26–32.

6 Art. 957a Abs. 3 des Bundesgesetzes betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (OR; SR 220).

7 Art. 959b Abs. 2 Ziff. 5 OR bei der Produktionserfolgsrechnung bzw. Abs. 3 Ziff. 3 bei der Absatzerfolgsrechnung.

8 Art. 959b Abs. 2 Ziff. 12 OR bei der Produktionserfolgsrechnung bzw. Abs. 3 Ziff. 6 bei der Absatzerfolgsrechnung.

9 Art. 959c Abs. 2 Ziff. 12 OR.

10 Vgl. «Neue Zürcher Zeitung» vom 28. Juni 2017, «Eine neue Schadsoftware greift Unternehmen weltweit an – und jetzt?» (https://www.nzz.ch/wirtschaft/not-petya-ein-neue-schadsoftware-befaellt-unternehmen-weltweit-und-jetzt-ld.1303222) und «20 Minuten» vom 28. Juni 2017, «Die Schweiz hat wegen Petya ein Päckli-Problem» (https://www.20min.ch/finance/news/story/Die-Schweiz-hat-wegen-Petya-ein-Paeckli-Problem-12909334).

11 Franz J. Kessler, in: veb.ch Praxiskommentar, 1. Aufl., Zürich 2014, Art. 959c N 89.

12 Basis: Art. 716a Abs. 1 Ziff. 2 und Ziff. 5 OR.

13 Zur Steuerpflicht von unsittlichen Erträgen siehe Urteil des Bundesgerichts 2C_426/2008 vom 18. Februar 2009, E 3.4. In wie weit auch Aufwände so behandelt werden könnten, lässt das Bundesgericht im Urteil 2C_916/2014 vom 26. September 2016, E. 7.6 offen.

[Rz 6] Zu prüfen ist somit, ob eine Strafanzeige gegen Unbekannt einzureichen und zugleich auch eine Meldung bei MELANI[14] vorzunehmen hilft, eine Beilage zum Buchungsbeleg vorzuweisen und zugleich ein Hinweis sein könnte, dass sich die betroffene Unternehmung um eine Aufklärung der Angelegenheit bemüht. Wer z. B. mittels einer lediglich vorgespielten Virus-Attacke – im Internet lassen sich problemlos Printscreens finden – Gewinne aus seiner Firma in eine schwarze Kasse verlagern möchte, wird das Risiko nach einer Strafanzeige aufzufliegen kaum in Kauf nehmen. Von Seiten der ESTV sind jedoch keine der beiden vorgenannten Schritte zwingend vorgegeben.

4. MWST-Folgen?

[Rz 7] Im Zusammenhang mit der MWST muss das Risiko, ob eine Bezugssteuer[15] geschuldet wird, abgeklärt werden. Würde man einen Software-Spezialisten im Ausland bitten, die Daten wieder lesbar zu machen und bei ihm eine entsprechende Software einkaufen, würden zweifelsohne die MWST-Folgen geprüft werden. Die Rechnung des Lieferanten müsste den Anforderungen von Art. 26 des Bundesgesetzes über die Mehrwertsteuer (MWSTG) entsprechen und zeigen, ob das ausländische Unternehmen in der Schweiz mit einer MWST-Nummer registriert ist.

[Rz 8] Nach einer Lösegeldzahlung wird je nach Art der Dateiverschlüsselung ein Code und ggf. eine Software zur Wiederlesbarkeit der Dateien übermittelt. Die Leistung des Erpressers unterscheidet sich kaum von der einer legalen Softwarelieferantin. Ob die Zahlung an eine im Inland tätige Organisation geleistet wird, lässt sich mangels Nachweis des Empfängers nicht beweisen. Die ESTV teilte hierzu mit, dass mangels Leistungswillen des Lösegeldzahlenden kaum mit MWST-Folgen zu rechnen wäre, im Einzelfall könnte jedoch je nach Gegebenheit trotzdem eine MWST geschuldet sein.

5. StGB-Risiko für den Lösegeldzahler?

[Rz 9] Wer einem Unbekannten wissentlich via Kryptowährung ein Lösegeld zukommen lässt, hilft bereits mit der Art der Zahlung mit, das Auffinden dieser Mittel zu vereiteln. Besteht das Risiko, dass der Unternehmung, welche das Lösegeld zahlt eine Untersuchung im Zusammenhang mit Geldwäscherei im Sinne von Art. 305bis des Strafgesetzbuches (StGB) droht? Mit der Kryptowährungsabbuchung ist die Lösegeldzahlung, anders als eine Barzahlung die zuerst z. B. auf ein Bankkonto eingeschleust werden muss, je nach Vorgehensweise von Beginn weg versteckt und nutzbar. Ob sich das Lösegeld in Kryptowährung wirklich vollständig verschleiern lässt, ist jedoch umstritten.[16] Bei strafrechtlichen Überlegungen muss zudem berücksichtigt werden, dass die das Lösegeld zahlende Unternehmung als Rechtfertigungsgrund einen Notstand geltend machen wird. Zu prüfen wäre trotzdem, inwieweit hier die Lösegeldzahlenden die Gefahr selbst in

14 Vgl. «Melde- und Analysestelle Informationssicherung MELANI» (https://www.melani.admin.ch/melani/de/home.html).

15 Art. 45 des Bundesgesetzes über die Mehrwertsteuer vom 12. Juni 2009 (MWSTG; SR 641.20).

16 Vgl. Klemens Kilic, «Wired» vom 4. Juni 2017, «Mit diesen 4 Schritten bleibt ihr im Bitcoin-Netzwerk anonym» (https://www.wired.de/collection/tech/wer-diese-vier-schritte-befolgt-bleibt-im-bitcoin-netzwerk-anonym) und Benedikt Fuest, «Die Welt» vom 8. Dezember 2017, «Der Bitcoin ist weniger anonym als gedacht» (https://www.welt.de/finanzen/article171408831/Der-Bitcoin-ist-weniger-anonym-als-gedacht.html).

pflichtwidriger Weise herbeigeführt haben und ihnen somit für die Notstandshandlung ein Vorwurf gemacht werden kann.[17] Das aktuelle Recht führt nicht mehr explizit auf, dass der Notstand nicht selbst verschuldet entstehen darf.[18] Es ist trotzdem davon auszugehen, dass ein Fall wie im alten Recht formuliert beurteilt werden sollte.[19] Eine Abklärung, ob eine Lösegeldzahlung wegen eines mangelhaft betreuten Computersystems erfolgte, könnte ein solches Selbstverschulden aufzeigen.

Würde jedoch z. B. eine Terror-Gruppe auf diese Art Geld generieren, könnte die Einschränkung in Art. 260^{quiquies}Abs. 2 StGB bei den Lösegeldzahlenden zu keiner Strafe führen. In Frankreich wird der Lafarge Holcim Konzern jedoch im Zusammenhang mit Schutzgeldzahlungen zur Sicherung ihrer Anlagen in Syrien die Finanzierung von terroristischen Vorhaben vorgeworfen (Bei diesem Fall handelt es sich nicht um Erpressung mittels Computerviren). Bei jeder Art von Erpressung einen Notstand geltend zu machen, ist somit nicht möglich.[20]

[Rz 10] Über eine Fallkonstellation im Sinne von Art. 102 StGB, bei der ein IT-Organisationsmangel zu einem Verbrechen oder Vergehen führte, welches keiner verantwortlichen Person zugeordnet werden konnte, und schlussendlich eine Busse zur Folge hatte, ist bis heute kein Urteil bekannt. Eine mangelhaft unterhaltene IT-Infrastruktur kann, schaut man auf die Häufigkeit von Presseberichten über Viren-Attacken, als ein in Kauf nehmen von einer solchen Attacke betrachtet werden. In Kauf nehmen wäre strafrechtlich gesehen ein Eventualvorsatz.[21] Wer sein Computersystem nicht ordnungsgemäss schützt nimmt in Kauf, dass sein System einem anderen System einen Schaden zufügt. Wird mit einem Botnetz[22] eine DDoS Attacke auf einen fremden Computer ausgeführt, können nicht nur Computer von Unternehmen, sondern auch ungeschützte Computer von Privatpersonen an der Attacke beteiligt sein. Der PC und die Gefährdungshaftung als neues Thema?

[Rz 11] Es ist möglich, dass trotz oder gerade wegen eines professionellen Umgangs mit der IT-Sicherheit, ein Computervirus sich auf einem System ausbreiten kann. Updates werden in einem professionell betreuten System zentral gesteuert. Ein Update mit einer aktualisierten Virusabwehr wird erst mit einigen Tagen Verzögerung aufgeschaltet, weil zuerst abgeklärt werden muss, ob dieses Update mit allen Anwendungen des Unternehmens kompatibel ist. Sonst riskiert das Unternehmen, dass es zwar einen Security-Update installiert hat, aber z. B. die Anwendung für die tägliche Kundenbearbeitung nicht mehr funktioniert. Gewisse Antimalware-Updates sollen jedoch nicht verzögert werden können.[23]

---

17 Andreas Donatsch, in: StGB Kommentar, 20. Aufl., Zürich 2018, Art. 18 Abs. 1 N 2 (zit. OFK/StGB-Autor).

18 Alt Art. 34 des Strafgesetzbuches vom 21. Dezember 1937 (StGB; SR 311.0): «… wenn die Gefahr vom Täter nicht verschuldet ist …».

19 Kurt Seelmann, in: Basler Kommentar Strafrecht I, 3. Aufl., Basel 2013, Art. 17 N 6.

20 Vgl. «Neue Zürcher Zeitung» vom 4. Dezember 2017, «Lafarge-Holcim räumt schwere Fehler in Syrien ein» (https://www.nzz.ch/wirtschaft/lafargeholcim-raeumt-schwere-fehler-in-syrien-ein-ld.1335361).

21 OFK/StGB-Donatsch, Art. 12 Abs. 2 N 3.

22 Botnetz = eine Gruppe von infizierten Rechnern die ferngesteuert werden können.

23 Vgl. «Neue Zürcher Zeitung» vom 28. Juni 2017, «Eine neue Schadsoftware greift Unternehmen weltweit an – und jetzt? Warum bringen Firmen ihre Software nicht auf den neusten Stand?» (https://www.nzz.ch/wirtschaft/notpetya-ein-neue-schadsoftware-befaellt-unternehmen-weltweit-und-jetzt-ld.1303222) und «Microsoft» vom 6. Januar 2018, «Deploy updates using Windows Update for Business» (https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb), Quality Updates mit Security Updates können um 30 Tage verzögert werden.

[Rz 12] Der mittels Virus oder DDoS erpressten Unternehmung ist klar, dass mit einer Zahlung eine kriminelle Organisation unterstützt wird. Der Reputationsverlust bei einem Bekanntwerden wird jedoch häufig als grösseres Problem betrachtet, und deshalb wird trotzdem bezahlt. Auch auf eine Strafanzeige wird verzichtet, weil man nicht die Polizei im Haus haben will. Die Lösegeldzahlung vom obenstehend beschriebenen Fall der Firma Uber wurde trotz Meldepflicht verschwiegen und erst ein Jahr später bekannt gegeben.[24]

6. Entwicklung der Gesetzgebung

[Rz 13] Die Gesetze werden in Zukunft genauere Vorgaben über die Behandlung solcher Erpressungsfälle enthalten. Das aktuell diskutierte Bundesgesetz über die steuerliche Behandlung finanzieller Sanktionen könnte etwas Klarheit im Zusammenhang mit widerrechtlichen oder unsittlichen Aufwänden schaffen[25]. Ein Postulat betreffend einer «Meldepflicht bei schwerwiegenden Sicherheitsvorfällen bei kritischen Infrastrukturen» wurde vom Nationalrat angenommen.[26] Der Bundesrat wird inzwischen für sein «mit angezogener Handbremse unterwegs» sein kritisiert.[27] Am 27. August 2018 wurde vom Bundesamt für wirtschaftliche Versorgung BWL ein IKT-Minimalstandard publiziert. Eine Pflicht zur Meldung von Vorfällen ist darin nicht enthalten. Die Publikation enthält Vorschläge zur Organisation der IT-Organisation und -Infrastruktur, um Cyber-Attacken zu verhindern. Die Ausführungen und Checklisten basieren auf internationalen Standards wie z. B. COBIT[28] und können als Best Practice Vorschlag betrachtet werden.[29]

[Rz 14] Wenn die Versorgung von Patienten in mehreren Spitälern wegen einem virenbefallenen System nicht mehr gewährleistet ist, spricht dies für eine generelle Meldepflicht.[30]Ebenso der Umstand, dass wegen eines Computervirus in Tschernobyl die Radioaktivität von Hand gemessen werden musste.[31] Die Folgen, wenn ein Computer nicht virenbedingt ausfällt, sondern stattdessen falsche Resultate anzeigt, könnten verheerend sein. Eine Meldepflicht kann die Verbreitung von Computerviren vielleicht frühzeitig behindern oder den Ursprung des Computerschädlings besser zurückverfolgen lassen. Mit der Pflichtmeldung hätte ein Unternehmen auch einen Beleg, der die steuerliche Abzugsfähigkeit der Lösegeld-Buchung begründen hilft.

---

24 Vgl. Eric Newcomer, «Bloomberg» vom 21. November 2017, «Uber Paid Hackers to Delete Stolen Data on 57 Million People» (https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data).

25 Botschaft zum Bundesgesetz über die steuerliche Behandlung finanzieller Sanktionen vom 16. November 2016, BBl 2016 8503.

26 NR Edith Graf-Litscher, Postulat 17.3475.

27 Lukas Mäder, «Neue Zürcher Zeitung» vom 18. Juli 2018, «Keine Zeit zum Zögern», S. 11 (https://zeitungsarchiv.nzz.ch/neue-zuercher-zeitung-vom-18-07-2018-seite-11.html).

28 Vgl. «ISACA» vom 17. Januar 2018, «COBIT Fact Sheet» (http://www.isaca.org/About-ISACA/Press-room/Documents/COBIT-Fact-Sheet_0318.pdf).

29 Vgl. «Bundesamt für wirtschaftliche Landesversorgung BWL» vom 27. August 2018, «IKT Minimalstandard» (https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html).

30 Vgl. Martin Linder, «Neue Zürcher Zeitung» vom 18. Mai 2017, «Wenn der Hacker Spitalpatienten mitbehandelt» (https://www.nzz.ch/digital/computervirus-wanna-cry-wenn-der-hacker-mitbehandelt-ld.1294555).

31 Vgl. «manager magazin» vom 27. Juni 2017, «Hacker-Angriff trifft Tschernobyl und Konzerne in Westeuropa» (http://www.manager-magazin.de/unternehmen/artikel/hacker-angriff-cyber-attacke-trifft-auch-maersk-saint-gobain-und-wpp-a-1154749.html).

7. Zivilrechtliche Folgen

[Rz 15] Unabhängig von den steuerlichen oder strafrechtlichen Fragen ist bereits heute mit Blick auf die möglichen zivilrechtlichen Folgen ein Unternehmen wie auch seine Organe gut beraten, die IT-Sicherheit laufend zu überwachen und die getroffenen Massnahmen zur Abwehr von möglichen Schäden zu dokumentieren.[32] Eine nachlässig organisierte IT-Kontrolle kann nicht mit einem «Innovationsstreben» oder einer «schöpferischen Risikobereitschaft» entschuldigt werden.[33] Ein Organ muss sich beraten lassen, wenn es in einem Bereich unerfahren ist, und auch mit dieser Beratung darf es sich «nicht blindlings» auf dieses Urteil verlassen».[34] Die Reederei Maersk musste wegen eines (ursprünglich von der NSA[35] hergestellten) Virus ihr ganzes Computersystem wiederherstellen. Der Schaden betrug USD 300 Mio.[36] Angesichts solcher Summen könnte ein Aktionär zurecht unbequem werden. Gut beraten ist, wer den Versicherungsschutz für das Unternehmen wie auch für dessen Organe abklärt.

[Rz 16] Die Postfinance übernimmt im E-Finance-Bereich bei finanziellen Schäden ihrer Kunden aus Phishing[37] bzw. Malware-Angriffen bis zu CHF 100'000 pro Fall.[38] Nicht gedeckt werden Schäden, die auf grobe Fahrlässigkeit des Kunden zurückzuführen sind. Dies dürfte wohl jene Kunden treffen, die kein Antivirusprogramm auf ihrem PC oder Smartphone installiert haben und trotzdem via einem solchen Gerät online arbeiten. Diese Einschränkung entspricht in Etwa dem Vorgehen bei einem Selbstverschulden, wie es im Zusammenhang mit dem Notstand thematisiert wurde.

Sikander von Bhicknapahari, lic.iur. / dipl. Experte in Rechnungslegung&Controlling, Freischaffend als Jurist und Controller, Dozent für Recht und Rechnungslegung an verschiedenen Instituten.

32 Urs Bertschinger, in: OR Kommentar, 2. Aufl., Zürich 2009, Art. 754 N 45 (zit. OFK-Autor).

33 OFK-Amstutz/Ramin, 3. Aufl., Zürich 2016, Art. 754 N3.

34 OFK-Amstutz/Ramin, 3. Aufl., Zürich 2016, Art. 754 N92.

35 Stefan Betschon, «Neue Zürcher Zeitung» vom 15. Mai 2017, «Noch nie wurden so schnell so viele Computer beschädigt» (https://www.nzz.ch/international/computersicherheit-cyberangriff-gefaehrdet-windows-pc-rund-um-die-welt-ld.1293201).

36 Vgl. «Handelszeitung» vom 16. August 2017, «Maersk macht Verlust wegen Cyber-Attacke» (https://www.handelszeitung.ch/unternehmen/maersk-macht-verlust-wegen-der-cyber-attacke-1463638).

37 Vgl. «Melde und Analysestelle Informationssicherung MELANI» vom 18. Mai 2015, «Physing» (https://www.melani.admin.ch/melani/de/home/glossar/phishing.html).

38 Vgl. «PostFinance» vom 20. August 2018, «Höchste Sicherheit im Online-Banking» (https://www.postfinance.ch/de/ueber-uns/medien/newsroom/medienmitteilungen/hoechste-sicherheit-onlinebanking.html).