RUHR-UNIVERSITÄT BOCHUM

RUB

RUBinform

Datenschutz & Datensicherheit

Newsletter 01|20

IN DIESER AUSGABE:

LINKS ZU DEN BEITRÄGEN:

www.rub.de/rubinform

ZUALLERERST

Liebe Leserinnen und Leser,

wir freuen uns, die erste Ausgabe der RUBinform in 2020 präsentieren zu können. Zwar mit etwas Verspätung und nur online, aber es sind auch wahrlich turbulente Zeiten. Kaum Corana-bedingt ins Home-Office umgezogen, begannen auch schon erste massive Spear-Phishing-Wellen, mit dem Resultat, dass zahlreiche Benutzeraccounts der RUB kompromittiert wurden. Durch die Cyber-Attacke im Mai verunsichert, haben sehr viele Nutzerinnen und Nutzer bei uns Rat gesucht, denn jeder Link in einer E-Mail und jedes komische Verhalten eines Systems standen plötzlich unter Verdacht – oft genug zu Recht. Wir danken auch all den Aufmerksamen intern wie extern, die wichtige Hinweise zu Sicherheitslücken gemeldet haben. *Bleiben Sie gesund!*

Stabsstelle für Informationssicherheit und behördlicher Datenschutz

ALLES **EMOTET?** – UNTERGRÜNDIGES

Im Jahr 2019 waren zahlreiche Unternehmen, Kliniken und öffentliche Einrichtungen von Totalausfällen oder zumindest großflächigen Ausfällen ihrer IT betroffen. Unter anderem waren dies die Heise Verlagsgruppe, die Städte Neustadt und Frankfurt, das Klinikum Fürth, das Kammergericht Berlin sowie die Universitäten Gießen und Maastricht. Ursache für die oft wochen- bis monatelangen Ausfälle waren Angriffe von Cyberkriminellen, die auch in 2020 unvermindert weitergehen: Dies musste leider auch die Ruhr-Universität im Mai schmerzlich erleben. Aber sind diese Ausfälle tatsächlich alle auf eine Infektion mit der Schadsoftware „Emotet" zurückzuführen, wie es sofort landauf, landab raunt, wenn derartige Vorfälle bekannt werden?

Was ist Emotet?

Dankeswerterweise sprechen einige der Betroffenen sehr offen über die Angriffe, damit andere die Chance haben, daraus zu lernen. Die Heise Verlagsgruppe und die Stadt Neustadt beispielsweise beschreiben ein mehrstufiges Verfahren, das die Angreifer angewandt haben:

Der initiale Zugriff auf das Netzwerk erfolgte über eine Spam-E-Mail, die im Anhang ein Office-Dokument mit Makros enthielt. Durch Ausführung der Makros wurde das Schadprogramm „Emotet" heruntergeladen und gestartet. Bei Emotet handelt es sich um einen Downloader, der auf einem infizierten System Outlook-Kontakte und -Korrespondenzen ausliest und diese an sogenannte Command-und-Control-Server (C&C-Server) ins Internet überträgt. Der Schadcode versendet sich anschließend an die ausgespähten Kontakte. Zur Generierung täuschend echt aussehender E-Mails werden Beziehungen zwischen Absender und Empfänger analysiert sowie Ausschnitte der Korrespondenz genutzt: Die gefälschten E-Mails sehen wie eine Antwort auf eine E-Mail aus, die der Empfänger selbst kürzlich an den Absender geschickt hat. Emotet besitzt ferner die Fähigkeit, sich lateral auf andere Systeme des kompromittierten Netzwerks auszubreiten und weiteren Schadcode nachzuladen. In den beschriebenen Fällen waren dies Trickbot und Ryuk.

Trickbot besitzt ausgefeilte Fähigkeiten, ein Netzwerk zu erkunden. Die „Befunde" werden an einen C&C-Server gesendet und dort von den Angreifern analysiert. Sobald interessante Ergebnisse dabei sind, beispielsweise ausgespähte Accounts mit weitreichenden administrativen Rechten und Zugriff auf sensible Datenbestände, schlagen die Angreifer zu: Daten werden abgezogen und mit Ryuk verschlüsselt. Den Code zum Entschlüsseln kann das Opfer gegen Zahlung von Lösegeld erwerben. Es wird aber auch gedroht, sensible Datenbestände zu veröffentlichen, wenn das Lösegeld nicht gezahlt wird.

Auch die Universität Maastricht gab auf einem Symposium Details zum Angriff bekannt und beschrieb ebenfalls ein mehrstufiges Verfahren: Der initiale Zugriff auf das Netzwerk erfolgte auch hier über eine Spam-E-Mail mit einem makrobehafteten Excel-Dokument im Anhang. Bei Ausführung der Makros wurde eine Malware namens SDBbot geladen. Mithilfe von SDBbot konnten die Angreifer weitere „legitime" Werkzeuge wie Meterpreter, PingCastle und PowerSploit nachladen. Diese Tools dienen zum Aufdecken von Schwachstellen innerhalb eines Netzwerks und werden auch von Sicherheitsfirmen genutzt. Dadurch waren die Angreifer an einen administrativen Account der Domain gelangt. Anschließend wurde die Ransomware CLOP ausgerollt.

An der Ruhr-Universität erfolgte der initiale Zugriff über einen übers Internet erreichbaren Remote Desktop Server.

Wer steckt dahinter?

IT-Sicherheitsfirmen haben tausende von Angriffen analysiert und können so die Vorfälle anhand der verwendeten Tools, Strategien und Techniken Gruppierungen von Cyberkriminellen zuordnen (siehe dazu auch Mitre Att&ck). Diese werden üblicherweise mit einem Codenamen bezeichnet, da in den wenigsten Fällen die tatsächlichen Akteure bekannt sind. Crowdstrike beschreibt im Global Threat Report 2020, dass es sich um arbeitsteilig arbeitende Banden handelt: Emotet wird demnach von einer Gruppe namens Mummy Spider „gepflegt" und anderen gegen anteilige Zahlung aus den Erpressungserlösen überlassen. Die Gruppe Wizard Spider entwickelt die Schadsoftware Trickbot und Ryuk und nutzt Emotet. Der Angriff auf Maastricht konnte von der analysierenden Sicherheitsfirma FOX-IT der Cybergang Threat Actor 505 (TA505) zugeordnet werden. Pinchy Spider ist eine Gruppe, die Ransomware an „Geschäftspartner" vermietet. Eine lukrative Angelegenheit: Pinchy Spiders Ransomware Gandcrab hat laut Angaben der Entwickler 2 Milliarden Dollar eingebracht. Im Mai 2019 gab die Gruppe bekannt, sich in den Ruhestand zu begeben. Allerdings scheinen sie mit der neuen Ransomware REvil alias Sodinokibi wieder durchzustarten. In einer forensischen Analyse von Revil fanden sich zwei Links auf Webseiten im Tor-Netzwerk: Eine Site dient als Auktionsplattform für die Daten aus den Einbrüchen. Für Daten aus einem Angriff auf eine New Yorker Anwaltskanzlei, die auch Prominente vertritt, werden 42 Millionen Dollar gefordert.

Generell ist laut Crowdstrike die Tendenz festzustellen, dass Angreifer nicht mehr nur auf automatisierte Ransomware Angriffe setzen, sondern Opfer gezielt aussuchen, um damit mögliche Erlöse zu steigern.

Cyber's Most Wanted

Für einige der Protagonisten lobt das FBI hohe Belohnungen aus: Für Hinweise zur Ergreifung von Maksim Viktorovich Yakubets ist eine Belohnung von bis zu 5 Millionen Dollar ausgesetzt. Er soll zusammen mit dem ebenfalls gesuchten Igor Olegowich Turashev die Cybergang EvilCorp anführen. Diese Bande steckt u.a. hinter dem Bankingtrojaner und Downloader Dridex und der Ransomware BitPaymer. Yakubets führt ein luxuriöses Leben in Russland. Er liebt speziell gestaltete Lamborghinis und große Feste. **BW**

Foto: iStock.com

ZEIT **AUFZURÄUMEN** – ZURÜCK IM BÜRO UND NOCH WEITER IM HOMEOFFICE

Nach dem spontanen Wechsel ins Home-Office ist für viele der heimische Schreibtisch der Mittelpunkt des Arbeitslebens geworden – die Erinnerung an den Büroarbeitsplatz ist nur noch dunkel vorhanden. Für die Anderen beginnt, zurück im Büro, endlich wieder die Zeit, in der man auch wieder was schafft und nicht konstant vom Päckchen für die Nachbarin oder Baustelle vor dem Haus von der Arbeit abgehalten wird. Mit dem Ende des „reduzierten Betriebs" an der RUB beginnt eine Phase in der Beschäftigte die Herausforderungen beider Arbeitsweisen meistern müssen. Nachdem viele Abläufe ohne große Planung und aus Mangel an Alternativen so eingerichtet werden mussten, gilt es nun Abläufe kritisch zu hinterfragen und auch mit Hinblick auf das kommende Semester die Abläufe solide zu gestalten.

Umgang mit Akten und Dokumenten

Im Home-Office sollten nur die Akten verfügbar sein, die unmittelbar zum Arbeiten benötigt werden. Das doppelte Ablegen von Akten und Dokumenten sollte vermieden werden und temporäre Kopien müssen sicher vernichtet werden. Soweit möglich sollte die Arbeit so geplant werden, dass Tätigkeiten, die entsprechende Zugriffe erfordern, im Büro erfolgen. Ein Vermischen von privaten und dienstlichen Dokumenten ist unbedingt zu vermeiden.

Digitale Infrastruktur

Sowohl zum Beginn der Pandemie als auch während des „RUB-Hacks" hatten schnelle Lösungen Priorität, um „erst mal wieder" erreichbar zu sein oder „mal eben" ein Dokument zusammen bearbeiten zu können. Benutzen Sie ausschließlich Ihre dienstliche E-Mail-Adresse zur Korrespondenz im Home-Office! Etwaige temporäre E-Mail-Adressen, Weiterleitungen an private Postfächer o.ä. sollten Sie abstellen. Seien Sie kritisch, wenn Sie Anfragen von Nicht-RUB-Adressen bekommen und geben Sie Informationen nicht einfach heraus.

Eine Checkliste mit vielen weiteren Informationen bietet das ULD Schleswig-Holstein und die BayLDA in ihren „Best Practices".

CHRISTOPHER **LENTZSCH,** INSTITUT FÜR ARBEITSWISSENSCHAFT

DIE CLEVERE ALTERNATIVE

Was ist ein Etherpad?

In der Reihe „Die clevere Alternative" stellen wir Online-Dienste vor, die an der RUB genutzt werden können und die eine Alternative zu gängigen Diensten großer Anbieter darstellen. Über die direkte Anmeldung mit der RUB-LoginID lassen sie sich einfacher in den Alltag der Hochschule einbinden und bieten zudem einen besseren Datenschutz. Die Nutzung für dienstliche Zwecke ist ebenso zulässig.

Etherpads können in der Lehre eine interessante Alternative zu anderen externen Echtzeit-Editoren sein. Ein Etherpad ist ein Texteditor, der aus einer Seite besteht, auf welcher gemeinsam geschrieben werden kann. Mehrere Personen können damit zeitgleich an einem Text arbeiten. Dieser wird automatisch synchronisiert und alle Änderungen sind direkt bei allen Teilnehmenden sichtbar. Etherpads lassen sich an der RUB in Moodle nutzen. Dort ist die Opensource-Software Etherpad Lite integriert. .

Funktionen

Das grundlegende Prinzip ist das gemeinsame Schreiben in Echtzeit. Die Beiträge der Teilnehmenden sind dabei mit verschiedenen Farben gekennzeichnet. Aus der Farbkodierung geht hervor, welcher Beitrag von wem stammt, und so kann die Übersicht einfach beibehalten werden. Die Autorschaft kann aber auch aufgehoben werden, wodurch das Etherpad anonymisiert wird. Neben dem eigentlichen Texteditor gibt es einen Chat, in dem sich die Teilnehmenden separat austauschen können, ohne dies in der eigentlichen Textbearbeitung tun zu müssen. Bereits vorgefertigte Texte können von Dateien ins Etherpad importiert und anschließend editiert werden. Gleichzeitig sind Etherpads als Ganzes exportierbar, wodurch die Inhalte nicht verloren gehen und Nachhaltigkeit geschaffen wird. Sie lassen sich so auch auf Webseiten einbinden.

Szenarien

Etherpad ist für die Lehre überall dort relevant, wo es um Austausch geht. Das gemeinsame Schreiben und Editieren von Texten eignet sich daher sehr gut für Gruppenarbeiten. Wenn beispielsweise Referate, die von mehreren Personen

zusammen gehalten wurden, verschriftlicht werden sollen, können die Studierenden ihren Teil verschriftlichen, ins Etherpad einfügen und anschließend die Teile ihrer Kommilitonen editieren. Das Etherpad eignet sich auch dazu, gemeinsam Informationen zusammenzustellen oder Ideen zu sammeln. Dadurch, dass alles in Echtzeit ist, kann sehr einfach gemeinsam Brainstorming betrieben und sofort auf die Beiträge der anderen Teilnehmenden eingegangen werden. Auch Online-Diskussionen oder Ergänzungen von Präsenzveranstaltungen sind mit dem Etherpad möglich. So sammeln die Studierenden zum Beispiel im Etherpad ihre Antworten auf eine zuvor gestellte Frage. Es können aber auch Fragen gesammelt werden, die während einer Präsenzsitzung unbeantwortet geblieben sind oder anonymes Feedback gegeben werden.

KATHRIN **BRAUNGARDT**, ANN KRISTIN **BECKMANN,** ZENTRUM FÜR WISSENSCHAFTSDIDAKTIK

DAS NEUE **RUB-DATACENTER**

Entsprechend der Bedeutung der IT für den Geschäftsbetrieb der RUB muss die erforderliche Hardware sicher betrieben werden. Mit Zustimmung der Ministerien hat die RUB daher den Bau- und Liegenschaftsbetrieb NRW mit dem Bau eines Datacenters beauftragt. Dieser hat Ende 2019 auf Basis eines Bieterwettbewerbs die Firma IBM als Generalübernehmer für die Planung und Erstellung des Datacenters beauftragt.

Errichtet wird ein hochverfügbares Datacenter nach Schutz-, Verfügbarkeits- und Effizienzklasse 3 der „Rechenzentrumsnorm" DIN EN 50600. Diese umfasst eine redundante Infrastruktur, hohe Schutzvorkehrungen und Maßnahmen zur Energieeffizienz. So wird das Datacenter bei Temperaturen unter 18°C komplett über Außenluft gekühlt. Um die Zertifizierung des Datacenters nach der Norm zu gewährleisten, wird bereits die Planung durch einen Zertifizierer begleitet.

Inzwischen ist der Bauantrag eingereicht. Im Spätherbst wird der Baugrund neben dem Technischen Zentrum der RUB gerodet. Die Fertigstellung des Datacenters ist im 4. Quartal 2021 geplant. Dann stehen schon im Erstausbau 72 umluftgekühlte und 6 wassergekühlte Serverracks für die Aufnahme der RUB-IT bereit.

RAINER **WOJCIESZYNSKI**

VIRUS TRIFFT **VIRUS**

IT-Sicherheit in Krisenzeiten

Besondere Zeiten - besondere Maßnahmen: Corona-bedingt mussten sich Studierende und Beschäftigte binnen kürzester Zeit auf die Arbeit im Homeoffice umstellen. Der Einsatz mobiler Systeme und privater Geräte führte zu neuen Arbeitsumgebungen und Abläufen. Gleichzeitig bahnten sich neue Gefährdungen an: dubiose Webseiten, die allerneueste Lageinformationen versprachen, aber Schadcode auslieferten, Videokonferenzen ohne Rücksicht auf Datenschutz, spezialisierte Angriffe per E-Mail oder Sicherheitslücken nach erleichterten Zugängen aus dem Homeoffice. Besonders die beiden letzteren hielten uns fortwährend in Atem.

Während sich Studierende und Beschäftigte Mitte März auf die Corona-bedingte Schließung und den Notfallbetrieb vorbereiteten, waren auch Cyber-Kriminelle nicht untätig: Zuvor erbeutete Kommunikationsinhalte und Zugangsdaten wurden für breit angelegte Angriffe ausgenutzt. E-Mails als Antwort auf bekannte Mail-Inhalte brachten Schadcode im Anhang mit oder lockten mit Download-Links. Die anfangs in verschlüsselten ZIP-Containern untergebrachten Schädlinge unterliefen so das Radar der Antivirus- und Spamanalyse an der RUB. Anhand der Analyse von Mail-Inhalten konnten wir Infektionen von Systemen und Accounts aufdecken.

Im April warnten Sicherheitsbehörden vor der Existenz von Benutzerkonten mit Trivial-Passwörtern auf RUB-Systemen, deren RDP-Zugänge aus dem Internet erreichbar waren. Die Existenz der Konten war zwar nicht verifizierbar – unserer Empfehlung, den RDP-Zugang zumindest auf das RUB-Netz zu beschränken, mochten dennoch nicht alle Systemadministratoren folgen. Seit dem Cyber-Angriff im Mai ist dies Historie. RDP ist auf dem Standard-Port nur noch aus dem RUB-Netz verfügbar.

Und immer wieder Phishing

Der Cyber-Vorfall im Mai traf Mail- und Exchange-Nutzer an der RUB unvorbereitet und eiskalt. Wer noch Zugriff auf seine Mailbox hatte, war oftmals unsicher, ob die eine oder andere Mail nicht gefährlich war. Jeder Link in E-Mails stand plötzlich unter Verdacht. Zwar konnten Exchange-Nutzer ihre E-Mails kurzfristig über RUB-Mail abwickeln und waren glücklicherweise schnell wieder erreichbar. Dennoch gab es heftige Auswirkungen auf das Mailsystem: die plötzliche Last verursachte Probleme für alle Nutzer, Exchange-Nutzer mussten sich an das Look-and-Feel von RUB-Mail gewöhnen. Es kam, was kommen musste: zahlreiche Phishing-Mails forderten zum Freischalten von E-Mails, Aktivieren von Konten oder Vergrößern von Mailboxen auf. Wer den Links folgte, landete auf gefälschten Webmail-Seiten. Eingegebene Zugangsdaten waren kompromittiert und wurden zum Spam-Versand in die ganze Welt missbraucht.

Was danach kommt

Um weitere Gefährdungen zu vermeiden, werden betroffene Accounts oder IT-Geräte in der Regel vorübergehend gesperrt. Deren Kompromittierung kann Meldepflichten auslösen (s. BITS-Box). Daher überprüfen wir in solchen Fällen, ob der Vorfall den Schutz personenbezogener Daten gefährdet hat.

Die automatisierte Analyse zur Ermittlung von Schadcode und Spam-Verhalten wird fortlaufend an die aktuelle Lage angepasst. Alle an RUB-Adressen gerichtete E-Mails passieren den zentralen Mailserver, werden dort gegebenenfalls abgewiesen oder als Spam klassifiziert. Die verwendeten Algorithmen aktualisieren ihre Regeln regelmäßig und automatisiert, neue Schädlinge oder Angriffsmuster werden aber nicht immer beim ersten Erscheinen erkannt.

Haben Sie unerkannte Schadcode- oder Spam-Mails erhalten oder gar die Spam-Filterung ausgeschaltet? Handeln Sie bitte stets umsichtig und überprüfen Sie vor dem Klicken auf Anhänge oder Links die Plausibilität der Inhalte. Bitte beherzigen Sie unsere Tipps und Videos zum Erkennen von bösartigen E-Mails und bleiben Sie sicher – auch in Krisenzeiten. **BS**

BITS

Meldepflichten

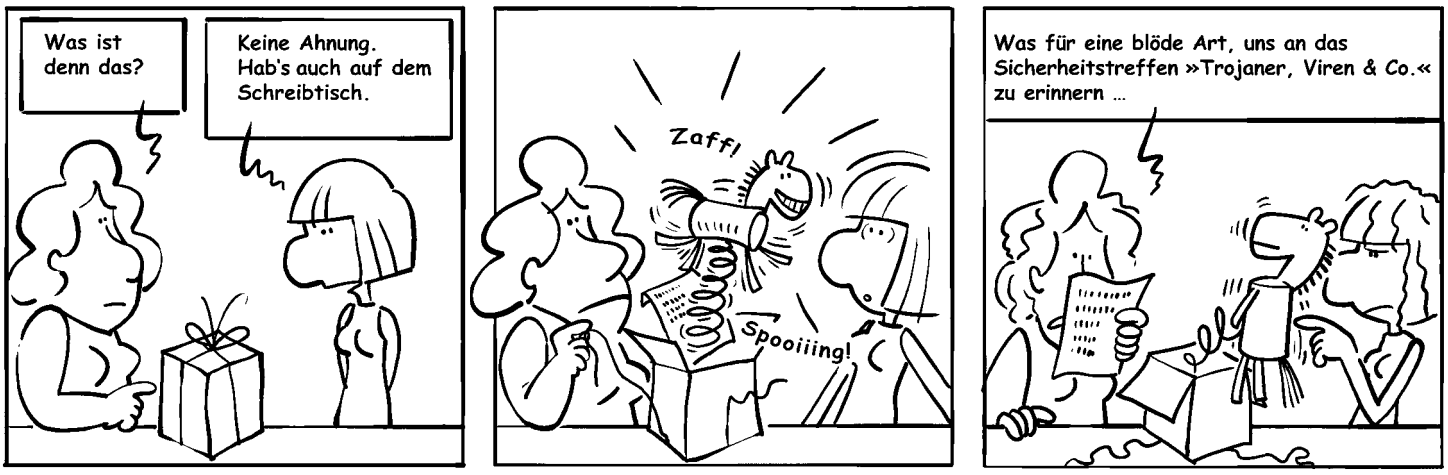
Die Ruhr-Universität ist gemäß Datenschutzgrundverordnung (DS-GVO) und anderen Datenschutz-Vorschriften für den sorgsamen Umgang mit den ihr anvertrauten personenbezogenen Daten verantwortlich. Dazu gehört auch die Datenschutz-Analyse nach Sicherheitsvorfällen oder Kompromittierung von Zugangsdaten sowie Rechnern Beschäftigter.

An der RUB sind der Datenschutzbeauftragte und die Stabsstelle für Informationssicherheit mit der Analyse und Veranlassung adäquater Maßnahmen beauftragt. Bitte melden Sie uns Vorfälle, bei denen eine Verletzung des Schutzes personenbezogener Daten möglich ist: Verlust oder Diebstahl von USB-Sticks, Datenträgern oder IT-Systemen, Ausspähung von Zugangsdaten, Verlust oder Fehlversand von Akten oder sonstigen Daten. Beispiele, Vordrucke und Abläufe schildert auch unsere Webseite *https://www.itsb.rub.de/themen/datenpanne.html*. **BS**

Mitre Att&ck

Mitre ist eine nicht-kommerzielle Organisation, die 1958 als Ausgründung aus dem Massachusetts Institute of Technology (MIT) entstanden ist. Sie betreibt zahlreiche von der US-Regierung finanzierte Forschungseinrichtungen mit dem Fokus auf öffentliche Sicherheit. Unter anderem verfügt Mitre über ein umfangreiches Cybersecurity Center. Dies ist bestens bekannt durch das Common Vulnerabilities and Exposures (CVE) System, eine standardisierte Liste über Schwachstellen in Computersystemen.

Mitre Att&ck ist eine riesige Wissensbasis, die Taktiken und Techniken von Cyberkriminellen aus zahlreichen Analysen von Angriffen klassifiziert. Sicherheitsteams lernen so die Vorgehensweisen von Angreifern besser zu verstehen und Schwachstellen in der Verteidigung ihrer Netzwerke aufzudecken. **BW**



HERAUSGEBER Dr. Kai-Uwe Loser (v.i.S.d.P.), KUL, Behördlicher Datenschutzbeauftragter der RUB (bDSB); Brigitte Wojcieszynski (v.i.S.d.P.), BW, Beauftragte für Informationssicherheit der RUB (ITSB); Birgit Steiner, BS, stellv. Beauftragte für Informationssicherheit der RUB (ITSB); Anschrift: Ruhr-Universität Bochum, Geschäftszimmer Stabsstelle Informationssicherheit, GAFO 04/622, Kerstin Bussmann, 44780 Bochum, Telefon: 0234/32-24888, E-Mail: rubinform@rub.de; Infos: www.rub.de/rubinform; Titelbild: ©KB

WEITERE INFOS
ZU UNSEREN THEMEN IM NEWSLETTER:

ALLES **EMOTET?** – UNTERGRÜNDIGES

Heise Verlagsgruppe und die Stadt Neustadt:

https://www.heise.de/ct/artikel/Was-Emotet-anrichtet-und-welche-Lehren-die-Opfer-daraus-ziehen-4665958.html

Universität Maastricht Symposium: *https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt*

Crwdstrike Global Threat Report 2020: *https://www.crowdstrike.de/ressourcen/reports/2020-crowdstrike-global-threat-report/*

Gandcarb retired: *https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/*

Sodinokibi: *https://blog.redteam.pl/2020/05/sodinokibi-revil-ransomware.html#!/2020/05/sodinokibi-revil-ransomware.html*

Auktionsplattform: *https://www.zdnet.de/88380475/revil-ransomware-gang-startet-auktionsseite-fuer-gestohlene-daten/*

Heise: *https://www.heise.de/security/meldung/Ransomware-Infektion-Ruhr-Universitaet-Bochum-ruft-zur-Passwortaenderung-auf-4721396.html*

Cyber's Most Wanted: *https://www.fbi.gov/wanted/cyber*

Dridex:

https://www.it-daily.net/it-sicherheit/cyber-defence/24004-top-malware-fuer-maerz-2020-dridex-stuerzt-emotet

https://www.infopoint-security.de/top-malware-fuer-april-2020-fernzugriffe-sind-stark-gefaehrdet/a23741/

https://www.itexperst.at/ransomware-bitpaymer-trifft-deutsches-unternehmen-fuer-automatisierungstechnik-12885.html

https://netzpalaver.de/2020/03/03/telekommunikations-branche-und-big-game-hunting-standen-2019-im-fokus-der-cyberkriminellen/

EvilCorp:

https://www.heise.de/newsticker/meldung/Dridex-Malware-Bislang-hoechste-Belohnung-fuer-Cyberkriminellen-ausgelobt-4606990.html

https://www.spiegel.de/netzwelt/web/fbi-schreibt-russische-hackergruppe-evil-corp-zur-fahndung-aus-a-1299951.html

Luxusleben: *https://arstechnica.com/information-technology/2019/12/members-of-evil-corp-the-cybercrime-group-that-lived-in-luxury-are-indicted/*

https://www.wired.com/story/alleged-russian-hacker-evil-corp-indicted/

ZEIT **AUFZURÄUMEN**

ULD Schleswig-Holstein*: https://www.datenschutzzentrum.de/artikel/1322-Ploetzlich-im-Homeoffice-und-der-Datenschutz-Die-Landesbeauftragte-fuer-Datenschutz-Schleswig-Holstein-informiert.html*

BayLDA: *https://www.lda.bayern.de/media/best_practise_homeoffice_baylda.pdf*

VIRUS TRIFFT **VIRUS**

Schadsoftware versteckt sich in ZIP-Archiven: *https://www.itsb.ruhr-uni-bochum.de/aktuelles/meldung00288.html*

Kompromittierung kann Meldepflichten auslösen: *https://www.itsb.ruhr-uni-bochum.de/themen/datenpanne.html*

Plausibilität erhaltener E-Mails überprüfen: *https://www.itsb.ruhr-uni-bochum.de/aktuelles/meldung00296.html*

Tipps und Videos zum Erkennen von bösartigen E-Mails:

https://www.itsb.ruhr-uni-bochum.de/themen/toptipps.html

https://www.itsb.ruhr-uni-bochum.de/themen/email_betrug.html

BITS

Mitre Att&ck *https://attack.mitre.org/*

Mitre Navigator *https://mitre-attack.github.io/attack-navigator/enterprise*

Mitre *https://en.wikipedia.org/wiki/Mitre_Corporation*