Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | **GEFÄHRDUNG** | VORFALL | IT-ASSETS

Auswirkungen von SARS-CoV-2 (Corona) auf die IT-Sicherheitslage

CSW-Nr. 2020-190290-1013, Version 1.0, 20.03.2020

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:GREEN: Organisationsübergreifende Weitergabe

Informationen dieser Stufe dürfen innerhalb der Organisation und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Die Auswirkungen von SARS-CoV-2 (Corona) durchdringen mittlerweile alle Lebensbereiche und machen auch vor der Informationstechnologie (IT) nicht halt. Die folgende Sammlung von Bedrohungen, Vorfällen und Ereignissen im Kontext der aktuellen Corona-Lage beschreibt unterschiedliche Angriffsszenarien, die derzeit verstärkt vom BSI beobachtet werden.

Generell muss davon ausgegangen werden, dass das Thema "Corona" bereits vermehrt bei Cyber-Angriffen aufgegriffen wird und eine steigende Entwicklung erfährt, da es

- für die gesamte Bevölkerung relevant ist und damit eine breite Masse adressiert,
- die aktuelle Unsicherheit in der Bevölkerung ausnutzt und
- Dringlichkeit in der Handlung vermittelt.

Beim Einfluss der Corona-Pandemie auf die IT-Sicherheit lassen sich unterschiedliche Wirkungsweisen unterscheiden:

- Ausnutzung des Themas für Social Engineering
- Desinformationskampagnen durch staatliche Akteure für eine generelle Destabilisierung werden aufgrund der Unsicherheitssituation einfacher
- die Risikobereitschaft der Bevölkerung wird aufgrund von Zeitüberschuss in Quarantäne einerseits und Zeitmangel oder Überlastung andererseits im kurzfristigen mobilen Arbeiten erhöht

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

- Angriffe auf das Gesundheitswesen allgemein und insbesondere auf die für Corona-Behandlungen zuständigen Stellen, zusätzlich im Bereich Logistik
- Ausnutzung der veränderten Bedingungen, die durch die Maßnahmen zur Bekämpfung der Corona-Lage entstanden sind. Dies sind insbesondere das

→ veränderte Verhalten der IT-Sicherheitsverantwortlichen und Anwender (z. B. vermehrte Telefon- und Videokonferenzen)
→ allgemein veränderter Gebrauch der IT-Infrastrukturen (z. B. wird die Unterscheidung von DDoS und vermehrten Nutzeranfragen schwieriger)
→ Ausnutzung der Versorgungslage sowie der finanziell angespannten Lage in davon besonders betroffenen Unternehmen/Industrien (z. B. könnten CEO-Fraud-Angriffe etc. im Online-Handel einfacher werden)
→ evtl. Abkürzung bzw. Vereinfachung von Workflows und Genehmigungsprozessen

Grundsätzlich lässt sich sagen, dass gegen die meisten Cyber-Angriffe die bisherigen IT-Sicherheitsempfehlungen schützen. Angriffskampagnen orientieren sich seit jeher an wesentlichen gesellschaftlichen Ereignissen und Themen. In diesem Fall wird lediglich die Corona-Lage als Aufhänger verwendet, wie es sonst mit anderen tagesaktuellen oder Neugier weckenden Ereignissen der Fall ist. Das durch die Corona-Lage verursachte öffentliche Interesse zieht sich durch alle Gesellschaftsschichten und betrifft sowohl das berufliche, als auch das private Leben.

Einfluss der Corona-Lage auf die IT-Sicherheit

DoS / DDoS-Angriffe

Denial-of-Service (DoS)-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (Distributed-Denial-of-Service). DDoS-Angriffe erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern (siehe https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817278).

Aktuelle Meldungen von DDoS-Angriffen:

- Link11: Anstieg von DDoS-Angriffen im Zusammenhang mit der Corona-Situation: https://www.totaltele.com/505216/Link11-Warns-of-30-Increase-in-Length-of-DDoS-Attacks-and-Disruption-Risks-as-Organizations-Accelerate-COVID-19-Remote-Working-Plans
- DDoS-Angriff auf die bayrische Lernplattform Mebis: https://www.heise.de/newsticker/meldung/Bayerische-Lernplattform-Mebis-von-DDoS-Angriffen-lahmgelegt-4683527.html
- DDoS-Angriff auf die Webseite des U. S. Health Department: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response
- DDoS-Angriff auf Lieferando: https://www.tz.de/wirtschaft/lieferando-deutschland-stoerung-angriff-lieferdienst-problem-keine-lieferung-corona-grund-zr-13605261.html

Im Allgemeinen werden die Aktivitäten im DDoS-Segment neben anderen hauptsächlich von zwei Aspekten geprägt:

- der Anzahl der zur Verfügung stehenden Ziele und
- dem Verhältnis zwischen dem Aufwand, den ein Angreifer für seinen Angriff aufbringen muss und dem Schaden, den er durch seinen Angriff erwartet.

Beide Aspekte sind durch die Corona-Schutzmaßnahmen, welche das Ziel einer möglichst umfangreichen Unterbrechung von Infektionsketten verfolgen, erhöht.

Maßnahmen zur Unterbrechung der Infektionsketten basieren auf dem Einhalten von physischen Abständen zwischen potenziellen Überträgern und potenziellen Neuinfizierten. Um unter diesen Umständen Geschäftsprozesse aufrechterhalten zu können, ist eine möglichst umfassende Virtualisierung wichtiger Geschäftsprozesse erforderlich. Hierzu gehören die Etablierung von Arbeitsmodellen wie dem mobilen Arbeiten genauso wie die vermehrte Durchführung von Video- und Telefonkonferenzen als Ersatz für Präsenzveranstaltungen.

Die Umsetzung dieser Maßnahmen bedeutet eine Exponierung der Unternehmen im Netz. Nicht nur die Anzahl der zur Verfügung stehenden Angriffsziele steigt hierdurch massiv an - auch der zu erwartende Schaden eines erfolgreichen Angriffs erreicht Ausmaße, die für Angreifer ein sehr lohnendes Aufwand/Schadensverhältnis ergeben. Der Schaden,

der sich für ein Unternehmen z. B. durch einen langanhaltenden erfolgreichen Angriff auf einen zentralen Server zum mobilen Arbeiten ergibt, in deren Folge die Geschäftsprozesse unmittelbar zum Erliegen kommen, kann derzeit existenziell sein, während sich ein ähnliches Angriffsszenario in Zeiten vor der Corona-Krise gar nicht zwingend ergeben hätte.

Für gering geschützte oder ungeschützte Unternehmen besteht bereits aufgrund der erhöhten Aktivitäten im Bereich der DDoS-Angriffe ein erhöhtes Risiko, Ziel eines Angriffs zu werden, gegen den kein adäquater Schutz besteht.

Für bislang bereits adäquat geschützte Unternehmen besteht derzeit kein unmittelbar erhöhtes Risiko, solange lediglich eine quantitative Zunahme der bekannten Angriffe erfolgt. Anders verhält es sich bei qualitativen Veränderungen, z. B. durch neue Angriffsvektoren oder DDoS-relevante Schwachstellen.

Hier besteht das Risiko, dass ein Angreifer durch einen erfolgreichen Angriff unter Anwendung eines bis dato unbekannten Angriffsvektors oder auf eine bislang unbekannte DDoS-relevante Schwachstelle aufgrund des beschriebenen situationsbedingt erhöhten Schadenspotenzials entsprechend massiv verstärkte Auswirkungen erzielen kann.

Seit Umsetzung der Schutzmaßnahmen gegen das Corona-Virus sind bislang noch keine neuen Angriffstechniken oder Schwachstellen beobachtet worden. Eine verstärkte Beobachtung in dieser Richtung ist derzeit jedoch aufgrund der angespannten Situation und des damit verbundenen erhöhten Schadenspotenzials besonders geboten.

Mögliche Maßnahmen

Das BSI empfiehlt die Beobachtung der nationale DDoS-Lage auf qualitative Veränderungen und verweist auf die Listen der qualifizierten Dienstleister (siehe https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/Qualifizierte_Dienstleister/QDL_node.html).

Schadprogramm-Verbreitung

Die Infektion eines Rechners oder Mobiltelefons erfolgt im Normalfall über den Versand von E-Mails, die Verbreitung von maliziösen URLs (z. B. über Social Media) oder die Manipulation von Lieferketten. In E-Mails können Anhänge mit Makros oder sonstigem ausführbaren Code enthalten sein. Durch die Ausführung des Schadcodes können Schwachstellen des Zielsystems ausgenutzt und/oder wiederum Schadprogramme nachgeladen und ausgeführt werden. Ebenso können durch den Aufruf von präparierten Webseiten Browser-Schwachstellen verwendet werden, um weitere Schadprogramme nachzuladen. Wird eine Lieferkette von Hard- oder Software manipuliert, können Schadprogramme bereits mit den ausführbaren Programmen (bzw. der App) installiert werden.

Die Schadprogramme können die verschiedensten Ziele verfolgen, sei es dass sie als Ransomware Dateien verschlüsseln und Erpressung ermöglichen, persönliche Daten ausspionieren oder als Bot-Komponente weitere zukünftige Aktionen unterstützen (z. B.DDoS-Angriffe, Spam-Versand etc.).

Durch die turbulente Nachrichtenlage, die leichte Emotionalisierbarkeit bei Gesundheitsthemen und ständig sich ändernden Anforderungen sind Opfer in der Corona-Krise leichter bereit Sicherheitsrisiken in Kauf zu nehmen oder sie aufgrund der Überforderung nicht wahrzunehmen. Die Neugierde und das Bedürfnis informiert zu sein führen auch dazu, dass potenziell mehr Software-Installationen durchgeführt und mehr Links geklickt werden, als evtl. notwendig wären.

Im Folgenden werden beispielhaft verschiedene detektierte aktuelle Schadprogramm-Kampagnen mit Corona-Bezug aufgelistet. Die Angst um den Corona-Virus wird hierbei ausgenutzt, um besorgte Opfer auf präparierte Webseiten zu locken oder dazu zu bringen, infizierte E-Mail-Anhänge zu öffnen bzw. schädliche Apps zu installieren. Nicht selten verwenden Angreifer dabei die echten Logos von Gesundheitsorganisationen wie z. B. der World Health Organization (WHO) bzw. von Gesundheitsministerien und -ämtern, wie dem US Center for Disease Control and Prevention (CDC). Es ist wahrscheinlich, dass diese Angriffe in Zukunft ausgeweitet werden und zusätzliche Organisationen (auch in Deutschland) im Bereich der Gesundheit bzw.

Regierungseinrichtungen dazu missbraucht werden, diese Schadprogramm-Kampagnen legitim wirken zu lassen. Zusätzlich birgt die Tatsache des verstärkten Einsatzes von Home-Office die Gefahr, dass Personen durch das erhöhte Aufkommen von E-Mails und Nachrichten sorgloser mit diesen umgehen und ihre Vorsicht vor Anhängen und maliziösen Links in Nachrichten verlieren:

- Eine Ransomware namens Corona-Virus ist aufgetaucht: https://www.bleepingcomputer.com/news/security/new-coronavirus-ransomware-acts-as-cover-for-kpot-infostealer/

- Android-Ransomware wird als angebliche Corona-Virus-Tracking-App zum Download auf einer Webseite angeboten: https://www.hackread.com/coronavirus-tracking-app-ransomware-scam-locks-phones-ransom/
- Remcos (Remote Access Trojaner): https://www.tripwire.com/state-of-security/security-data-protection/attack-campaign-leveraged-coronavirus-theme-to-deliver-remcos-rat/
- Corona-Virus wird in Schadprogramm-Spamwellen verwendet, sowie in Verbindung mit schadhaften Domainnamen, welche neu registriert wurden: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains
- FormBook-Trojaner per Spam-Kampagne versendet: https://securityaffairs.co/wordpress/99156/cyber-crime/coronavirus-spam-campaign.html
- Bereits im Januar dieses Jahres ist eine Schadprogramm-Kampagne mit Emotet bekannt geworden: https://www.govinfosecurity.com/fake-coronavirus-messages-spreading-emotet-infections-a-13675
- Schadprogramme, die über eine vermeintliche Corona-Geokarte verbreitet werden: https://t3n.de/news/malware-verseuchte-vorsicht-1261675

Die Bedrohung durch fortschrittliche Angriffe, wie EMOTET (Banking-Trojaner, der u. a. E-Mail-Adressen und -Inhalte ausspäht), TRICKBOT (Banking-Trojaner mit Funktionen zur Kompromittierung gesamter Windows-Domänen) und RYUK (Ransomware) können kurzfristig wieder akut werden und in der besonderen Lage besonders schwere Konsequenzen haben. Die empfohlenen Schutzmaßnahmen sind weiter mit Nachdruck umzusetzen (vgl. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/Ransomware/Ransomware_node.html).

Social Engineering

Beim Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst, Dringlichkeit oder Respekt vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. Das zentrale Merkmal von Angriffen mithilfe von Social Engineering besteht in der **Täuschung über die Identität** und **die Absicht des Täters**. Der Angreifer verleitet das Opfer auf diese Weise beispielsweise dazu, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadprogramme auf dem privaten Gerät oder einem Computer im Firmennetzwerk zu installieren.

Phishing

Beim Phishing wird versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen. Dazu werden z. B. gefälschte E-Mails und/oder Webseiten-URLs verbreitet. Wird diese Manipulation vom Opfer nicht erkannt und die Authentizität einer Nachricht oder Webseite nicht hinterfragt, gibt das Opfer seine Zugangsdaten u. U. selbst unwissentlich in unberechtigte Hände (siehe https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817302). Die Unsicherheit im Umfeld der Maßnahmen zu Corona, der reale und empfundene Zeitdruck und die Fokussierung auf das eine bestimmende Thema führen dazu, dass bei der Prüfung weniger Sorgfalt an den Tag gelegt wird, oder dass Personen mit der Bearbeitung von E-Mails oder der verstärkten Nutzung von Webseiten beauftragt werden, die dies normalerweise nicht tun. Folgende exemplarische Fälle sind dem BSI in diesem Umfeld bekannt:

- Deutschsprachige Corona Phishing-E-Mails wurden im Phishing-Radar der Verbraucherzentrale NRW registriert: https://www.verbraucherzentrale.nrw/aktuelle-meldungen/digitale-welt/achtung-phishing-wie-betrueger-die-coronakrise-in-emails-nutzen-45714
- Hinter einem Informationsauftritt zu Corona verbarg sich ein Schadprogramm (Info-Stealer): https://blog.malwarebytes.com/social-engineering/2020/02/battling-online-coronavirus-scams-with-facts/
- Phishing-E-Mails im Namen des Centers for Disease Control and Prevention wurden verbreitet (CDC, dt. Zentren für Seuchenkontrolle und -prävention): https://www.kaspersky.com/blog/coronavirus-phishing/32395/
- Neben Phishing-E-Mails kursieren derzeit vor allem Spam-E-Mails mit Angeboten für Desinfektionsmittel und Atemschutzmasken
- EMOTET nutzt für seine Angriffe abgeflossene Original-E-Mails von Kommunikationspartnern. Diese sind besonders authentisch und verleiten zu dem Anklicken der Links bzw. dem Öffnen von präparierten Dokumenten.

Derzeit häufen sich die Vorfälle, in denen sich Angreifer die aktuelle Lage zunutze machen, um Phishing-Kampagnen vor dem Hintergrund der aktuellen Corona-Pandemie zu starten. Dem BSI wurden auch deutschsprachige Phishing-E-Mails gemeldet, die sich dadurch auszeichnen, dass sie sprachlich sehr gut sind, gezielt mit Emotionen spielen und das

aktuell bestimmende Thema Corona adressieren. Das dabei gewählte Vorgehen der Angreifer unterscheidet sich jedoch grundsätzlich nicht von früheren Kampagnen.

Nach Analysen von Check Point wurden seit Januar 2020 über 4.000 Domains mit Corona-Bezug registriert. Die Wahrscheinlichkeit, dass dies mit krimineller Absicht geschah (Phishing oder Schadprogramme) sei größer als bei anderen Domains, die im selben Zeitraum registriert wurden. Dies gilt auch im Vergleich zu anderen Registrierungen mit Bezug zu saisonal relevanten Themen der letzten Zeit, die ebenfalls häufig von Kriminellen als Vorwand verwendet wurden, wie beispielsweise zu dem Valentinstag (siehe https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/).

CEO Fraud & Betrug durch vermeintlichen Microsoft-Support

Beim CEO Fraud versuchen kriminelle Täter Entscheidungsträger bzw. für Zahlungsvorgänge befugte Mitarbeiter oder Mitarbeiterinnen in Unternehmen so zu manipulieren, dass diese vermeintlich im Auftrag des Managements Überweisungen von hohen Geldbeträgen veranlassen. Beim Betrug durch einen vermeintlichen Microsoft-Support versuchen hingegen angebliche Mitarbeiter des technischen Supports von bspw. Microsoft per Telefon oder über gefälschte Warnhinweise, Sicherheitsfunktionen auszuhebeln oder Schadprogramme auf dem Rechner des Opfers zu installieren (siehe https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IT_Sicherheit_am_Arbeitsplatz/SoEng/Social_Engineering_node.html). Beide Methoden treffen in der aktuellen Sondersituation u. U. vermehrt auf unvorbereitete oder unaufmerksame Personen, die sich gezwungen sehen, hier schnell zu handeln, ohne die gebotenen Überprüfungen durchzuführen.

- Dem BSI liegen aktuell keine Informationen zu konkreten CEO Fraud Angriffen und den Betrug durch vermeintlichen Microsoft-Support im Kontext von "Corona" vor, jedoch gibt es häufig Warnungen davor (z. B. https://www.interpol.int/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19) und es ist davon auszugehen, dass Handlungen in dieser Kategorie durchgeführt werden, auch ohne dass Meldungen dazu bekannt sind.

Die grundsätzliche Ausnahme-/Überlastsituation in den Unternehmen, das verteilte Arbeiten, die motivierte Kurzfristigkeit von Maßnahmen (kurzfristiger Erwerb von Schutzmasken, Desinfektionsmitteln etc.) bzw. durch Corona verursachte Umsatzeinbußen steigern aktuell die Verwundbarkeit für CEO Fraud Angriffe und den Betrug durch vermeintlichen Microsoft-Support. Durch eine panische Schnellreaktion werden ggfs. die erhaltenen Anfragen (per E-Mail oder Telefon) nicht weiterführend geprüft oder hinterfragt.

Mögliche Maßnahmen

- Teilen Sie Passwörter, Zugangsdaten oder Kontoinformationen niemals per Telefon oder E-Mail mit. Banken und seriöse Firmen fordern ihre Kunden nie per E-Mail oder per Telefon zur Eingabe bzw. Herausgabe von vertraulichen Informationen auf.
- Lassen Sie bei Anfragen über digitale Medien besondere Vorsicht und Ruhe walten: Sollte auch nur ansatzweise der Verdacht bestehen, dass es sich um einen Angriffsversuch handeln könnte, reagieren Sie im Zweifelsfall besser überhaupt nicht oder versichern Sie sich über einen getrennten Kanal über die Richtigkeit eines Anliegens.
- Prüfen Sie bei E-Mails besonders, ob es sich bei dem Absender um eine legitime Mail-Adresse handelt. Behalten Sie jedoch im Kopf, dass sich der Absender leicht fälschen lässt. Eine allgemein gehaltene Anrede sowie die in der E-Mail enthaltenen Links geben aufschlussreiche Hinweise über die Korrektheit einer Nachricht.
- Sensibilisieren Sie Ihre Mitarbeiter/-innen im Umgang mit E-Mails und Telefonanrufen. Informieren Sie Ihre Mitarbeiter über aktuell bekannt gewordene Phishing-E-Mails.

Weiterführende Informationen:

- https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IT_Sicherheit_am_Arbeitsplatz/SoEng/Social_Engineering_node.html
- https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Themen/Social_Engineering/social_engineering_node.html
- https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrdungen/G_0_42_Social_Engineering.html

- https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/ORP/Umsetzungshinweise_zum_Baustein_ORP_3_Sensibilisierung_und_Schulung.html

Angriffe auf und über existierende VPN-Zugänge

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft des Internets) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptographischer Verfahren die Integrität und Vertraulichkeit von Daten über öffentliche Netze geschützt und die Kommunikationspartner sicher authentisiert werden.

Der Begriff VPN wird oft als Bezeichnung für verschlüsselte Verbindungen verwendet, zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls (siehe https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817314).

Aufgrund der aktuellen Situation senden immer mehr Unternehmen ihre Mitarbeiter/-innen nach Hause, um von dort zu arbeiten. Hierfür stellen die Unternehmen in der Regel VPN-Zugänge zur Verfügung, damit die Mitarbeiter/-innen mittels Fernzugängen Zugriff auf das Unternehmensnetzwerk bekommen und dessen Dienste nutzen können. Ein DDoS-Angriff auf VPN-Dienste eines Unternehmens könnte somit ein lohnendes Ziel für Cyber-Kriminelle sein. Die entsprechende Absicherung dieser Dienste gegen Angriffe dieser Art ist daher wichtig (siehe DoS/DDoS).

Grundsätzlich sollten zur Absicherung die referenzierten Maßnahmen beachtet werden. Neben der erfolgreichen Authentifizierung des Benutzers, der Absicherung des Endgeräts und des Arbeitsplatzes im Allgemeinen und des Einsatzes eines kryptographisch gesicherten VPNs gehört dazu die Umsetzung konkreter technischer Empfehlungen wie z. B. die Verwendung von Zwei-Faktor-Authentisierung (2FA) und/oder Benutzer- und System-Zertifikaten. Des Weiteren sind die Protokolle der verwendeten VPN-Dienste zu prüfen, also bspw. OpenVPN (UDP 1194) oder SSL VPN (TCP/UDP 443, IPsec/IKEv2 UDP 500/4500). Anhaltspunkte für einen potenziellen Missbrauch könnten z. B. eine Häufung von Fehlversuchen oder die erfolgreichen Logins von ungewöhnlichen IP-Adress-Geolokationen sein. Selbiges gilt auch für alternative Fernzugriffs-/Fernwartungszugänge (bspw. RDP, SSH, TeamViewer oder LogMeIn). Von einer Verwendung unverschlüsselter Protokolle (z. B. Telnet oder VNC) für die Fernwartung über öffentliche Netze wird explizit abgeraten.

- Mögliche Angriffe auf VPN Netzwerke https://thehill.com/policy/cybersecurity/487542-hackers-find-new-target-as-americans-work-from-home-during-outbreak

Mögliche Maßnahmen

- Beachtung der Umsetzungshinweise im IT-Grundschutz Kompendium

→ Sicherer Fernzugriff: https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Fern/fern_node.html
→ VPN: https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-VPN/vpn_node.html

- Weitere Tipps zur Absicherung von Remote-Zugängen

→ https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely
→ https://securitymadein.lu/news/covid-19-safety-and-cybersecurity-can-go-hand-in-hand/
→ https://www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit

Angriffe auf webbasierte Office-Anwendungen

Um von zu Hause arbeiten zu können, nutzen Unternehmen verstärkt auch Cloud-basierte Office-Anwendungen. Grundsätzlich ist zunächst die Erreichbarkeit von Cloud-Diensten ein kritischer Faktor. Netz/-Rechenzentrumsausfälle oder DDoS-Angriffe können die Verfügbarkeit gefährden. Im Gegensatz zu VPN-Lösungen muss in der Praxis häufig keine sichere Fernzugriffssoftware eingerichtet werden. Dennoch sind zur Verhinderung von unauthorisierten Zugriffen verschiedene Absicherungsmaßnahmen zu berücksichtigen, da z. B. Phishing-Angriffe für die Cloud-Dienste drohen. Einen wirksamen Schutz bietet hier etwa die Nutzung einer Zwei-Faktor-Authentifizierung (2FA).

Mögliche Maßnahmen

- Microsoft Office 365

→ Schutz gegen Phishing und Datenverlust: https://www.kyberturvallisuuskeskus.fi/en/office-365-email-phishing-and-data-breaches-very-common-detect-protect-inform

- Google G-Suite

→ Sicherheits-Checkliste für mittlere und große Unternehmen: https://support.google.com/a/answer/7587183?hl=de
→ Sicherheits-Checkliste für kleine Unternehmen: https://support.google.com/a/answer/9211704?hl=de

Advanced Persistent Threats (APT)

Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen teils sehr hohen Ressourceneinsatz und oft erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren (siehe https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817272).

Das BSI hat Kenntnis darüber, dass mehrere Gruppen in den letzten Wochen sogenannte Köderdokumente verwendet haben, die vorgeben, Informationen über den Corona-Virus zu enthalten. Entscheidend für die Lageeinschätzung ist dabei, dass die Gruppen ihre gewohnten Ziele angreifen und ihre etablierten Angriffstechniken verwenden.
Das BSI sieht bei gezielten Angriffen bisher keine massive Verschärfung der IT-Sicherheitslage, da keine neuen Angriffstechniken verwendet und keine neuen Zielgruppen angegriffen werden. Für Einrichtungen, die bereits im Fokus von gezielten Angriffen standen, steigt jedoch die Wahrscheinlichkeit, dass bei Empfängern die Neugier über die Vorsicht siegt und Köderdokumente geöffnet werden. Es gelten weiterhin die Empfehlungen des BSI, die die Erfolgswahrscheinlichkeit solcher Angriffe verringern.

Das BSI hat bisher keine Kenntnis über gezielte E-Mail-Angriffe in Deutschland, die Köderdokumente mit Corona-Bezug benutzten. IT-Sicherheitsfirmen berichten jedoch über Tätergruppen aus unterschiedlichen Weltregionen, die das Corona-Thema für Social Engineering bereits gegen Ziele in Osteuropa, Zentral- und Südostasien einsetzen.

Verbreitung von Fake-News

Der Begriff Fake-News setzt sich aus zwei Begriffen zusammen. "Fake" heißt "gefälscht" und "news" heißt "Nachrichten". Es sind also gefälschte Nachrichten. Mit reißerischen Schlagzeilen, gefälschten Bildern und Behauptungen werden so Lügen und Propaganda verbreitet. Fake-News erwecken den Eindruck, dass es sich um echte Nachrichten handelt (siehe https://www.bpb.de/nachschlagen/lexika/das-junge-politik-lexikon/239951/fake-news). Die Verunsicherung über Corona führt zu massenhaft Falschmeldungen und Gerüchten sowie zu Fake-News. Um diese Nachrichten glaubhaft wirken zu lassen werden ebenfalls Floskeln wie "aus zuverlässiger Quelle" verwendet:

- Falsche Zahlen in Corona-Karte nach Hackerangriff https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware
- Panikmache per WhatsApp https://www.tagesschau.de/faktenfinder/panikmache-coronavirus-101.html
- Gefälschte medizinische Produkte werden mit Bezug zu Corona in den Umlauf gebracht https://www.interpol.int/News-and-Events/News/2020/Global-operation-sees-a-rise-in-fake-medical-products-related-to-COVID-19

Mögliche Maßnahmen

- Quelle der Meldung prüfen (Ist diese ein bekanntes und renommiertes Medium?, Handelt es sich um eine offizielle Quelle?)
- Verwendung eines "Fakten-Checks" aus einer bekannten und renommierten Quelle, z. B. https://www.tagesschau.de/faktenfinder/
- Auch in Zeiten der Krisen auf den gesunden Menschenverstand verlassen

Allgemeine Informationen von (internationalen) Behörden

- https://www.bbk.bund.de/DE/TopThema/TT_2020/TT_Covid-19.html
- Beispielhafte Warnung der Kollegen aus Österreich: https://www.bmi.gv.at/news.aspx?id=7745347A7971512F6968343D

- Australian Cyber Security Centre's COVID-19 advice: https://www.cyber.gov.au/news/cyber-security-essential-when-preparing-covid-19
- https://www.link11.com/de/blog/presse/corona_virus_oeffentlicher_sektor_schutz_cyber-attacken_kostenlos/

Länderspezifische Vorfälle

Aus den folgenden Ländern liegen dem BSI Einzelberichte vor. Parallel laufen die Aktivitäten auf EU-Ebene. Relevantes fließt in die Lagebeobachtung und -bewertung sowie die Produkte des BSI ein.

Polen

In Polen wurden Schadprogramm-Kampagnen festgestellt, die auf die Bankdaten der Bürgerinnen und Bürger zielen. Zu den Kampagnen gehören:

- Versand von Phishing-SMS (Thema: Bezahlung zum Impfschutz)
- Versand von Phishing-SMS (Verlinkung auf Fake-Behördenwebseite)
- Spendenaufrufe

Slowakei

- https://www.sk-cert.sk/en/warning-against-malicious-phishing-campaigns-related-to-coronavirus/index.html
- https://www.sk-cert.sk/en/security-recommendations-of-the-national-cyber-security-centre-sk-cert-for-operators-of-essential-services-regarding-to-covid-19-updated-measures/index.html

Mögliche Szenarien, Prognose und Bewertung

Die im Abschnitt "Einfluss der Corona-Lage auf die IT-Sicherheit" beschriebenen Vorfälle und Szenarien können, obwohl sie zum Teil international und deren Opfer sich in unterschiedlichen Ländern befanden, jederzeit auch in Deutschland eintreten.

Es ist sehr wahrscheinlich, dass Cyber-Angriffe in den nächsten Wochen und Monaten international und in Deutschland zunehmen werden.

Folgende von den im Abschnitt "Einfluss der Corona-Lage auf die IT-Sicherheit" abweichend bzw. abgewandelte Szenarien können eintreten:

- Durch die zunehmende Nutzung von Home-Office, VPN und Cloud-Anwendungen, wird die IT innerhalb von Unternehmen einer größeren Belastung ausgesetzt. Unternehmen, in denen Home-Office bislang nicht angeboten wird, müssen ggf. ihre IT noch darauf vorbereiten und Beschaffungen tätigen. Bei diesen ad-hoc Änderungen an der IT-Infrastruktur, die in aller Regel sofort und unverzüglich umgesetzt werden müssen (Firewalls, VPN-Zugänge, etc.), könnten Unternehmen durch Konfigurationsfehler Lücken entstehen, die Angreifer ausnutzen können. Es ist auch möglich, dass Angreifer zukünftig gezielt nach offenen Ports in Firewalls scannen. Darüber hinaus sollten diese Änderungen an der IT regelmäßig überprüft, nach Überwindung der Corona-Krise wieder rückgängig gemacht und unter einem ständigen Monitoring stehen. Den Unternehmen muss außerdem bewusst werden, dass durch die kurzfristig eingeleiteten Maßnahmen gewisse Geschäftsbereiche (hier die IT im Besonderem) unter Umständen zusätzliches Personal benötigt, um sowohl den laufenden Betrieb zu erhalten, als auch die neu eingerichteten Zugriffsmöglichkeiten zu administrieren und einzurichten. Zusätzliche Hinweise zu Home-Office gibt folgende BSI-Seite: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/HomeOffice/homeoffice.html
- Da jeder potenziell zur Zielgruppe gehört, müssen Cyber-Kriminelle ihre Angriffskampagnen nicht mehr umständlich zielgruppengerecht anpassen, sondern können die breite Masse adressieren. Hierbei ist jede öffentliche Neuigkeit und das Interesse der Menschen daran, zum Beispiel über mögliche Maßnahmen gegen den Virus oder Neuigkeiten über etwaige Ausbreitungen sowie Heilmittel zugleich Input und ein Aufhänger für Kriminelle, diese zugleich als Einfallstor zu nutzen. Zielgruppengerechte Aufbereitung in Form von CEO-Fraud sind selbstverständlich nicht ausgeschlossen.

Grundsätzlich gibt es keine neuen Bedrohungen der IT-Sicherheit als vor der Corona-Pandemie. Durch die nunmehr geänderte Arbeitsweise in den Unternehmen und Behörden, sollten alle Maßnahmen, die Unternehmen,

Privatpersonen und Behörden treffen, nicht überstürzt/unvorsichtig getroffen werden. Durch die zunehmende Flut an E-Mails und die Berichterstattung über Corona sollte die Vorsicht vor maliziösen Links und Anhängen nicht außer Acht gelassen werden. Kriminelle werden diesen Zustand in den nächsten Wochen und Monaten weiterhin ausnutzen.

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

   Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.