Managementzusammenfassung IT-Sicherheit in der Corona-Pandemie

BSI 2020-190290

Erstellt durch:
Südwestfalen-IT
Sonnenblumenallee 3
58675 Hemer

IHR KONTAKT

Auskunft erteilt: Marc Risse

Durchwahl: +49 2372 5520 385

Zentrale: +49 2372 5520 0

Fax: +49 2372 5520 279

Email: risse@citkomm.de

Inhalt Seite

Dokumentenhistorie

Was?	Wer	Version	Inhalt
Erstellung	Risse	0.2	
Qualitätssicherung	MiNe	0.3	Kürzungen, Hervorhebungen, Review. Neuer Status: vorgelegt
Qualitätssicherung	Rombach	0.4	Redaktionelle Änderungen

1. BSI-Meldung zur Corona-Pandemie

Die anliegende Mitteilung des BSI gibt umfangreiche Hinweise zu Risiken und Maßnahmen für die öffentliche IT im Rahmen der Corona-Pandemie. Die folgende Zusammenfassung ist als Service für die IT-Verantwortlichen gedacht. Sie soll die Umsetzung und Einordnung der Maßnahmen erleichtern.
Dieser Text enthält keine Empfehlungen, Wertungen oder Einordnung der Maßnahme im Kontext der SIT. Hinsichtlich der fachlichen Korrektheit wurden seitens der SIT keine eigenen Untersuchungen angestellt. Bei Widersprüchen zwischen Texten sind stets die Aussagen des BSI zu verwenden.

2. 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.
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.

3. Einfluss der Corona-Lage auf die IT-Sicherheit

3.1. DoS / DDoS-Angriffe

Dieser Punkt wird hier nicht behandelt, weil dies eine Aufgabe der SIT ist. **Kommunen mit eigenen Internetzugängen (VPN, Citrix) sollten diesen Punkt im BSI Papier beachten.**

3.2. Schadprogramm-Verbreitung

Schadprogramme können auf unterschiedlichen Weg ins Unternehmen gelangen. Dieser Infektionsweg führte bereits in der Vergangenheit zu großflächigen Ausfällen. 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 Softwareinstallationen durchgeführt und mehr Links geklickt werden, als evtl. notwendig wären.

3.3. 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.

3.4. 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. 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. Es werden unerfahrene Personen mit der Bearbeitung von E-Mails oder der Nutzung von Webseiten beauftragt.
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.

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) ist größer als bei anderen Domains, die im selben Zeitraum registriert wurden.

3.5. CEO Fraud und 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. 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.

3.6. 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.
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.

3.7. 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 unautorisierten 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).

3.8. 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 (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.

4. Mögliche Szenarien, Prognose und Bewertung

Es ist sehr wahrscheinlich, dass Cyber-Angriffe in den nächsten Wochen und Monaten international und in Deutschland zunehmen werden. Folgende 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. Bei diesen ad-hoc Änderungen an der IT-Infrastruktur, die in aller Regel sofort und unverzüglich umgesetzt werden müssen (Firewalls, VPN-

Zugänge, etc.), könnten in **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.

- 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. Eine zielgruppengerechte Aufbereitung in Form von CEO-Fraud ist selbstverständlich nicht ausgeschlossen.

5. Fazit

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. **Gleichzeitig gilt es das Sicherheitsniveau auf dem aktuellen Stand zu halten und nicht durch unbedachte IT-Maßnahmen zu gefährden.** 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.