ALTHAMMER & KILL

Informationssicherheit in der Corona-Krise:

Die Corona-Krise wirkt sich auch auf die Gefährdung von Organisationen und Unternehmen durch kriminelle Bedrohungen aus. Während das Vorkommen bestimmter Delikttypen in der Krise offensichtlich eher abnimmt, passen sich Täter an und erweitern ihre Modi Operandi. Organisationen und Unternehmen müssen sich im Zusammenhang mit COVID-19 vor teilweise aufwendig vorbereiteten Angriffen durch Cyber-Kriminelle schützen.

Aktuell scheint sich insbesondere der Gesundheitssektor im Fokus der Täter zu befinden. Die derzeitige Fokussierung interner Ressourcen auf die COVID-19 Krisenbewältigung darf nicht zu Schäden durch einen Rückgang an Security-Awareness und Gefahrenbewusstsein innerhalb der Belegschaft führen.

Neue Angriffsvektoren von Cyber-Kriminellen

Die Corona-Krise verändert das Kriminalitätslagebild in Deutschland, die Einschränkungen des öffentlichen Lebens führen gegenwärtig offenbar zu einem Rückgang im Teilbereich der Straßenkriminalität. Verschiedene Entwicklungen zeigen jedoch, dass die aktuelle Lage zu einem veränderten IT-Sicherheitslagebild und angepassten Vorgehensweisen, z.B. bei Betrugsdelikten, führt. So wird das Corona-Virus und die damit einhergehende Betroffenheit bei Entscheidungsträgern und Mitarbeitern genutzt um Viren, Ransomware und Verschlüsselungstrojaner zu verbreiten oder an persönliche Daten zu gelangen. Insbesondere Organisationen, Unternehmen und Einrichtungen des Gesundheitssektors scheinen sich aktuell im Fokus der Täter zu befinden.

Durch falsche Angebote und Hinweise zum Umgang mit Corona in Text oder Betreffzeile der E-Mails soll der Nutzer dazu bewogen werden, auf einen kompromittierten Link zu klicken. Angepasst wurde auch die bekannte Tatbegehungsweise des CEO-Fraud; hier werden Entscheidungsträger aufgefordert, Lieferungen wie z.B. medizinische Geräte, Schutzmasken oder Desinfektionsmittel zeitnah im Voraus zu bezahlen.

Ein weiteres Betrugsrisiko besteht durch sogenannte „Fake Shops“, in denen relevante und derzeit kaum verfügbare Produkte angeboten werden. Bei diesen Fake Shops handelt es sich um Nachbauten existierender Online-Shops oder in Betrugsabsicht aufgebaute Web-Präsenzen nicht existierender Unternehmen, die Lieferung wird durch den Kunden bezahlt aber nicht zugestellt.

Aufgrund der konspirativen Vorgehensweise durch Täter und der Nutzung von Möglichkeiten zur Anonymisierung im Internet gestaltet sich die Strafverfolgung dieser Täter schwierig und überwiesene Beträge sind häufig nicht zurückzuerhalten. Die Täter beziehen die hohen Belastungen von Mitarbeitern in der aktuellen Situation bewusst in ihre Tatvorbereitung ein; die außerordentlich hohe Stressbelastung darf nicht zu einem Rückgang der Security-Awareness und des Gefahrenbewusstseins innerhalb der Belegschaft führen.

Version 2

Sicherheitsempfehlungen für die E-Mail-Nutzung:

- **Vorsicht bei E-Mails** von unbekannten Adressen, die z.B. Links mit Informationen zu aktuell diskutierten Aspekten wie z.B. Video-Konferenzen enthalten.
- **Klicken Sie nicht** auf den verdächtigen Link und öffnen Sie auf keinen Fall entsprechende Anhänge.
- Führen Sie **Downloads** immer nur aus den **Originalquellen** und entsprechend der **intern geltenden Vorgaben** durch.
- Seien Sie grundsätzlich **misstrauisch**, wenn Sie **persönliche Daten** übermitteln sollen.
- Der Absender nutzt **keine Absende-Adresse des genannten Unternehmens**, die Absende-Adresse ist fehlerhaft oder es gibt sonstige Auffälligkeiten; prüfen Sie den **E-Mail-Header** zur Verifikation.
- Prüfen Sie **Text** und **Signatur** des Absenders.
- Wurde die E-Mail durch bestehende Präventionsmaßnahmen als **auffällig** klassifiziert?
- Unterhalten Sie überhaupt eine **Geschäftsbeziehung** zu z.B. der Bank oder dem Unternehmen?
- Seien Sie auch bei **persönlichen Anreden** in der E-Mail überaus vorsichtig.

Hinweise zum Erkennen von Fakeshops:

- Kaufen Sie nur bei **bekannten Anbietern** ein, bei denen entsprechende Erfahrungswerte vorliegen.
- Überprüfen Sie **Impressum, Domain, Anschrift, AGB** und **handelnde Personen**.
- Führen Sie Maßnahmen zur **Verifikation des Anbieters** durch.
- Die **Preise für die Ware** sind außerordentlich **niedrig** und können nur per **Vorkasse** bezahlt werden.
- Begehrte Produkte sind **permanent verfügbar**.
- Der Onlineauftritt ist **unvollständig** und/oder **fehlerhaft**; Teile der Seiten beinhalten **keinen Inhalt**.
- Die **Domain ist fehlerhaft**.

Denken Sie daran:
Melden Sie jegliche Verdachtsfälle umgehend Ihrem Informationssicherheitsbeauftragten, dem Datenschutzbeauftragten oder wenden Sie sich vertraulich an Althammer & Kill.