Up to Data: Der Cyber-Angriff

Vielleicht haben Sie es in den Nachrichten gehört:

HACKER-ANGRIFF BEI LEBENSMITTELHÄNDLER

Zu Beginn der Woche teilte der Lebensmittelhändler Tegut – mit Hauptsitz in Fulda – mit, dass sein IT-Netzwerk von Hackern angegriffen worden sei. Auf der Firmen-Website heißt es, dass man „alle IT-Netzwerk-Systeme der Zentrale gemäß dem bestehenden Notfallplan habe herunterfahren und vom Netz nehmen können." Das Unternehmen habe daraufhin die zuständige Sicherheitsbehörde informiert.

Dieses Szenario beschreibt den „Worst-Case" eines Unternehmens. Aber was ist zu tun, wenn ein Unternehmen Opfer eines Cyber-Angriffs wird? In diesem Newsletter erfahren Sie überblicksartig, was ein Cyber-Angriff ist, welche Möglichkeiten der Schadsoftware es gibt und wie man sich schützen kann.

1. Was ist überhaupt ein Cyber-Angriff

Als Cyber-Angriff wird ein gezielter Angriff auf ein oder mehrere informationstechnische Systeme bezeichnet, der zum Ziel hat, die IT-Systeme durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen. Der Angriff findet dabei ausschließlich im virtuellen Cyber-Raum statt. Bei Cyber-Angriffen kommen hauptsächlich Schad- oder Spähsoftware zum Einsatz (z.B. Trojaner, Viren – zur Unterscheidung siehe unten).

Aufgrund von meist hoch entwickelten Schadprogrammen, sind Abwehr- und Rückverfolgungsmöglichkeiten häufig begrenzt. Dadurch können oft keine Rückschlüsse auf Identität und Hintergründe des Angreifers gezogen werden. Theoretisch kann jeder Computer, der mit einem Netzwerk verbunden ist, Opfer einer Cyber-Attacke werden.

Passiert ein solcher Cyber-Angriff, ganz gleich durch welche Schad-Software er ausgelöst wurde, ist dies als Datenpanne zu behandeln.

2. Welche schadhaften Programme gibt es?

Grundsätzlich sind sämtliche Schadprogramme unter dem Begriff „Malware" zu sammeln. Diese Programme können beispielsweise so ausgestaltet sein, dass sie das Löschen oder die Manipulation von Daten, die technische Kompromittierung von Sicherheitseinrichtungen oder das ungefragte Abgreifen von Daten zum Gegenstand haben.

Hier erhalten Sie einen groben Überblick und daher nicht abschließenden Überblick über die bekanntesten Varianten der Malware:

Viren	➢ Werden meist über Dateifreigaben, Web-Downloads oder E-Mails in Umlauf gebracht ➢ Ein Virus ist ein bösartiger Code, der die Funktionsweise eines Computers verändern und schädliche Wirkung erzielen kann
Würmer	➢ Würmer können sich ohne menschliche Interaktion in Netzwerken vervielfältigen ➢ Hierdurch ist eine schnelle Ausbreitung möglich
Trojaner	➢ Sind dafür konzipiert, sensible Daten in Netzwerken ausfindig zu machen und so die Kontrolle über das infizierte System zu übernehmen
Spyware	➢ Dient dem unbekannten Erfassen von Eingaben, sowie Verhaltens- und Nutzungsmustern
Adware	➢ Wird zur Verbreitung von Werbung verwendet, welche dem Angreifer Gewinn einbringt

3. Wie kann ich mich schützen?

Um sich vor Cyber-Attacken zu schützen, gibt es mehrere Maßnahmen, die Unternehmen kumulativ gewährleisten sollten.

- Sensibilisieren Sie Ihre Mitarbeiter im Umgang mit Downloads und E-Mail-Anhängen
- Schulen Sie Ihre Mitarbeiter regelmäßig in diesen Bereichen
- Es sollten grds. alle bereitgestellten Sicherheitsupdates von Software- und Anwendungsherstellern zeitnah installiert werden
- Deaktivierung von Makros in Office-Programmen
- Technisch-organisatorische Maßnahmen mit IT abstimmen (Erstellung eines Notfallplans, Firewall, Virenschutz, Erstellung von BackUps)
- Netzsegmentierung

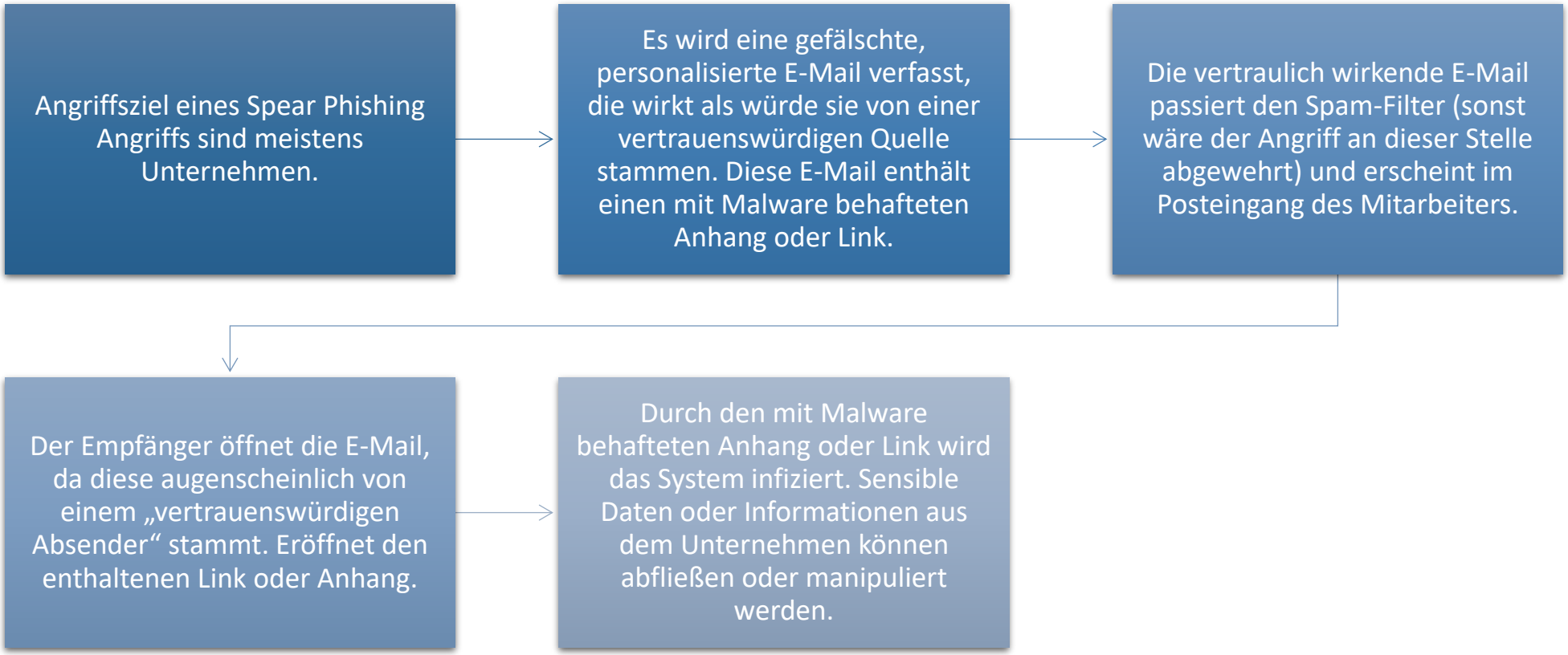
4. Was tun, wenn es zu spät ist

Wenn Sie – wie Tegut – Opfer eines Cyber-Angriffs geworden sind, sollten Sie Ihren IT-Fachmann und auch den Datenschutzbeauftragten einbeziehen. Der IT-Fachmann unterstützt Sie dabei, dass Ihre Systeme wieder einsatzfähig werden und die etwaigen Ausfallzeiten möglichst niedrig gehalten werden. Der Datenschutzbeauftragte ist ebenfalls miteinzubinden, da ein Cyber-Angriff eine (meldepflichtige) Datenpanne darstellt.

Wichtig ist es dann, eng mit dem Datenschutzbeauftragten und der IT zusammen zu arbeiten, damit zeitnah eine Meldung an die Behörde nach den Vorschriften der DSGVO erfolgen kann. (Achtung: Hier gilt eine 72-Stunden-Frist). In einem zweiten Schritt ist dann zu prüfen, ob auch Kundendaten durch den Angriff abhandengekommen sind. Wenn Sie diese Frage mit „ja“ beantworten können, dann müssen die Betroffenen ebenfalls über den Vorfall informiert werden. Es muss in diesem Falle eine Meldung sowohl an die Behörde, als auch an die Betroffenen erfolgen.

5. Sonderproblem: Spear Phishing

Zudem gibt es unter den Cyber-Angriffen noch das – für Unternehmen wohl relevanteste – Problem des sog. „Spear Phishings“.



Sollten Sie zu diesem Themenbereich weitere Fragen haben, stehen wir Ihnen jederzeit gerne zur Verfügung.

Ihr Team der RKM Data GmbH