# Gut vorbereitet ist schon halb gewonnen

*Unternehmen, die sich intensiv auf einen Cyberangriff vorbereiten, haben deutlich weniger mit den Folgen der Attacken zu kämpfen.*

Cybersecurity konzentriert sich hauptsächlich auf die Prävention. Und das geht am besten durch Lernen aus Vorfällen. Dennoch passiert es Unternehmen immer wieder, dass sie attackiert werden. In einem solchen Fall geht es darum, den Schaden zu minimieren und so viel wie möglich aus den bekannten Erfahrungen zu lernen. Was also ist die „best Practise“?

**Mit einem Plan ist viel gewonnen**

Einen Plan für die Reaktion auf einen Vorfall (Incident Response, IR) legt das IT-Security-Team die Maßnahmen fest, die im Falle einer Sicherheitsverletzung oder einem Angriff greifen müssen. Folgende Fragestellungen sind die Grundlage für einen IR-Plan:

- Wie schwerwiegend ist der Vorfall?
- Wo befinden sich die kritischen Systeme und wie sind sie zu isolieren?
- Wie und mit wem soll kommuniziert werden?
- Wer ist zu kontaktieren und welche Maßnahmen sind zu ergreifen?
- Was ist mit den Sicherheitskopien?

Dabei sollte ein IR-Plan einfach und überschaubar sein, damit er in einer Situation mit hohem Druck leicht zu befolgen ist. Das SANS Incident Handler's Handbook und der Incident Response Guide von Sophos können bei der Planerstellung sehr hilfreich sein.

**Hilfe anfordern**

Bevor es nach einem Angriff darum geht, Computer und Systeme wiederherzustellen oder gar ein Lösegeld auszuhandeln, sollten Unternehmen Hilfe anfragen. Die Reaktion auf Angriffe erfordert spezielle Fähigkeiten, und die meisten Unternehmen beschäftigen keine Incident-Response-Spezialisten.

Ein Plan beinhaltet die Kontaktdaten von IR-Dienstleistern. Wenn sich der Angriff gegen Server und Endgeräte richtet, z.B. bei einem Ransomware-Vorfall, sollte zunächst der Anbieter für die Endpoint-Sicherheit kontaktiert wenden, insbesondere wenn dieser einen IR-Dienst anbietet. Er verfügt wahrscheinlich über Telemetriedaten der betroffenen Umgebung und hat Zugang zu vorinstallierten Tools wie EDR/XDR, mit denen er schnell helfen kann.

**Hilfe ausweiten**

Es ist ratsam, sich an die örtlichen Strafverfolgungsbehörden zu wenden. Mit hoher Wahrscheinlich ist mit dem Vorfall ein Verbrechen begangen worden, und möglicherweise verfügen die entsprechenden Behörden über hilfreiche Ressourcen.

Selbstverständlich muss der Vorfall auch bei der Versicherungsgesellschaft für Cybersicherheit angemeldet werden, sofern eine Versicherung besteht. Im Falle einer Zusammenarbeit mit einem Technologieanbieter oder Systemintegrator kann dieser möglicherweise bei der Wiederherstellung helfen, z.B. bei den Backups.

**Isolieren und eindämmen**

Der Vorfall sollte so gut wie möglich isoliert und eingedämmt werden. Dazu gehört auch das Ausschalten der Stromversorgung, das Trennen der Internetverbindung und das Trennen der Netzwerke, eine softwarebasierte Isolierung, die Anwendung von Deny-All-Firewall-Regeln und das Herunterfahren kritischer Systeme. Sollte ein noch funktionsfähiger Domänencontroller zur Verfügung stehen, gilt es, diesen wenn möglich zu erhalten, indem man den Server herunterfährt und/oder vom Netz trennt. Auch Backups sollten isoliert und

vom Netzwerk getrennt sein. Darüber hinaus gilt es alle mutmaßlich kompromittierten Kennwörter zu ändern und die Konten zurückzusetzen.
Wichtig beim Einsatz von Incident-Response-Diensten, ist die Beratung darüber, wie betroffene Systeme und Verbindungen wieder in Betrieb genommen werden können.

**Kein Lösegeld zahlen**
Zwar klingt die Zahlung des Lösegelds nach einem „einfachen“ Ausweg, ermutigt die Kriminellen aber zu weiteren kriminellen Taten. Außerdem sind die Zeiten moderater Lösegeldforderungen längst vorbei: Der Sophos State of Ransomware Report 2021 zeigt, dass mittelständische Unternehmen im vergangenen Jahr durchschnittlich 147.000 Euro Lösegeld gezahlt haben. Die Sophos-Studie ergab auch, dass nur 65 Prozent der verschlüsselten Daten nach einer Lösegeldzahlung wiederhergestellt werden konnten und mehr als ein Drittel der Daten trotzdem verloren war.
Zudem ist die gesetzliche Lage bei Lösegeldzahlungen weltweit unterschiedlich. Es ist deshalb ratsam, sich über etwaige Gesetze in dem Land (oder den Ländern) zu informieren, in dem eine Organisation tätig ist.

**Beweise aufbewahren**
Allzu oft passiert es, dass Opfer von Attacken hauptsächlich damit beschäftigt sind, ihre Systeme und Dienste so schnell wie möglich wiederherzustellen. Dabei gehen viele Informationen verloren, die dabei helfen würden, die Ursache zu ermitteln und das Ausmaß der Sicherheitsverletzung zu verstehen. Diese können jedoch einem Incident-Response-Team Aufschluss darüber geben, mit wem sie es zu tun hat und welche Taktiken diese Gruppe üblicherweise anwendet. Sie könnte sogar einen ganz neuen Stamm von Ransomware und die verwendeten Taktiken, Techniken und Verfahren (TTPs) offenbaren.
Die Aufbewahrung der Images von Systemen und virtuellen Maschinen ist ebenso wichtig, wie die isolierte Speicherung der Malware. So können Unternehmen auch im Falle einer gerichtlichen Prüfung von Versicherungsansprüchen Beweise vorlegen oder gegenüber einer staatlichen Stelle nachweisen, dass sie nicht gegen Offenlegungsvorschriften verstoßen haben.

**Gegner und Vergeltung**
In vielen Fällen stecken mehrere Gruppen hinter einem Ransomware-Angriff. Beispielsweise mit den Informationen aus der Lösegeldforderung und den Gemeinsamkeiten in den Taktiken, Techniken und Verfahren (TTPs) kann ein erfahrenes Incident-Response-Team in der Regel schnell erkennen, mit wem sie es zu tun haben. Vom Versuch der Vergeltung, dem so genannten „Hack Back", wird hingegen dringend abgeraten. Er ist wahrscheinlich von vornherein illegal und kann die Situation nur noch verschlimmern.

**Die Rolle der Cyberversicherung**
Bei einem Cyberangriff, der durch eine Cyberversicherung abgedeckt ist, wird ein Schadensregulierer der Versicherungsgesellschaft zunächst einen externen Rechtsbeistand beauftragen. Dieser organisiert interne und externe Ressourcen und koordiniert die Aktivitäten bis zur Behebung des Vorfalls.
Es lohnt sich, beim Abschluss einer Versicherung im Voraus zu klären, welche Aktivitäten und welche spezialisierten Anbieter im Falle eines Cyberangriffs abgedeckt sind. Die meisten Cyber-Versicherungen akzeptieren die Nutzung bereits bestehender Dienstleister.

**Kommunikation aufrechterhalten**
Die Kommunikation wird durch Cyberangriffe oft schwer beeinträchtigt. E-Mail-Systeme sind möglicherweise offline, elektronische Kopien von Versicherungspolicen oder IR-Pläne sind verschlüsselt und der Angreifer überwacht möglicherweise die Kommunikation. Daher ist es ratsam, eine alternative Kommunikationsmöglichkeit bereitzuhalten, z.B. eine Instant-Messaging-Anwendung. Mit einem separaten Kanal können das gesamte Team und alle anderen Beteiligten kommunizieren. Versicherungsdaten, IR-Pläne und Kontakte zu den IR-Spezialisten sollten gesondert und in physischer Form aufbewahrt sein.

**Neu: Social Media von Sophos für die Presse**
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

**Pressekontakt:**

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de