IT-NOTFALLPLAN:
IM FALLE EINES CYBER-ANGRIFFS BESTENS GEWAPPNET

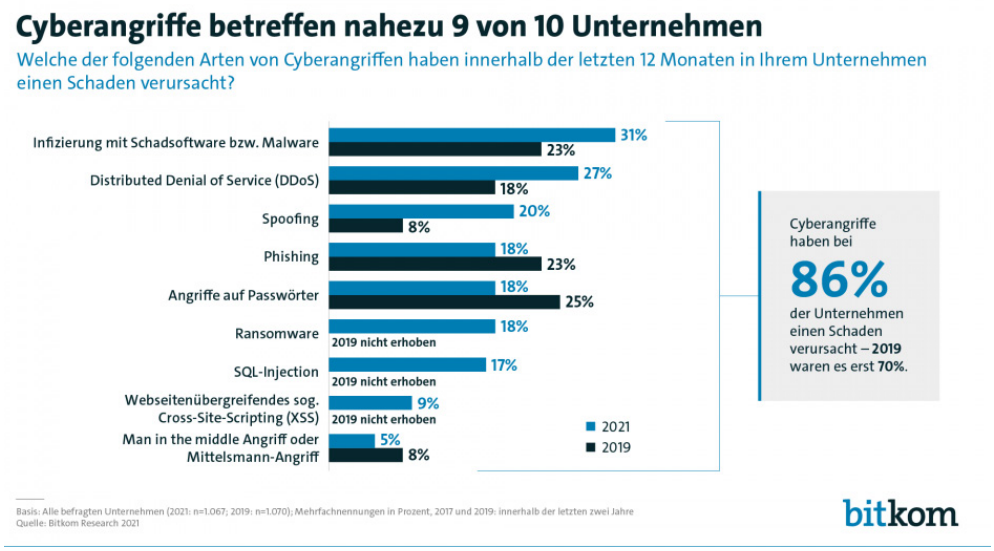
Da ist es passiert: Auf einmal gingen alle Rechner in den Ruhemodus, die Webseite war down und keiner der Mitarbeiter war in der Lage, auf das Netzwerk oder die Daten zuzugreifen. Es war der Tag, an dem die komplette IT in einem mittelständischen Betrieb plötzlich stillstand. Wie sich herausstellte für die nächsten vier Wochen, denn auf solch einen Vorfall war das Unternehmen nicht vorbereitet.

Und was tun, wenn das Kind in den Brunnen gefallen ist? Viele Organisationen sind auf solch einen Krisenfall nicht gefasst. Firmenlenker erkennen die Notwendigkeit eines Notfallplans immer mehr, doch es hapert an der Umsetzung. Laut einer im Jahre 2019 durchgeführten Studie des eco-Verbandes verfügen 57 Prozent der befragten Unternehmen über interne Prozesse respektive einen Notfallplan für den Fall eines erfolgreichen Cyber-Angriffs. Weitere 27 Prozent arbeiten an einem solchen Krisenkonzept. Im Vergleich zu 2018 konnten nur 32 Prozent auf einen Notfallplan zurückgreifen. Die Studie offenbart darüber hinaus, dass diese „Baustelle" aktuell zu den Top-Sicherheitsthemen gehört: 80 Prozent bewerten einen Notfallplan als wichtig oder sogar sehr wichtig.

Und wie sieht es im Jahr 2021 aus? Laut einer aktuellen Umfrage von Statista besitzen gerade einmal 60 Prozent der Teilnehmer einen Notfallplan. Diese Steigerung zu 2019 erscheint nicht nur sehr gering, sie offenbart noch etwas anderes: Wenn das Risk Management denn mal vorhanden ist, wird es nicht regelmäßig aktualisiert. 42,8 Prozent der befragten KMU haben Notfallpläne in den Schubladen liegen, aber kümmern sich nur unregelmäßig um notwendige Updates.

Deutsche Unternehmen zu wenig für den Krisenfall gewappnet

Experten bewerten dieses Verhalten als fahrlässig. Längst ist nicht mehr die Frage, ob digitale Angriffe kommen werden – sondern wann es passieren wird. Dies belegt eine Umfrage des Digitalverbandes Bitkom, die im August 2021 veröffentlicht wurde. Fast 90% der 1.000 befragten Unternehmen aus allen Branchen gaben an, von Cyberangriffen betroffen gewesen zu sein. Durch Spionage, Sabotage und Diebstahl entstand der deutschen Wirtschaft jährlich ein Gesamtschaden von 223 Milliarden Euro (2020/21) – doppelt so hoch wie in 2018/19.



Quelle Bitkom: Umfrage aus dem Jahr 2019 und 2021 im Vergleich www.bitkom.org

Erste Schritte zu einem effektiven Notfallplan

Die „Goldene Stunde" nennen Experten aus der Akut- und Notfallmedizin die entscheidende Phase bei lebensgefährlichen Verletzungen oder Erkrankungen. Je schneller reagiert wird, desto besser stehen die Chancen auf eine vollkommene Genesung. Als Voraussetzung für eine erfolgreiche Goldene Stunde im betrieblichen Kontext gilt ein professionelles Notfall-Management („Business Continuity Management"). Das Ziel ist, die Ausfallsicherheit der Prozesse zu erhöhen und in einem Notfall systematisch und schnell zu reagieren - gerade bei Hackerangriffen und Malware-Attacken.

Der auch als IT-Störungsmanagement bzw. IT Incident Management benannte Notfallplan umfasst typischerweise den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Störungen in IT-Bereichen sowie hierzu vorbereitende Maßnahmen und Prozesse. Das Spektrum möglicher Vorfälle reicht dabei von technischen Problemen und Schwachstellen bis hin zu konkreten Angriffen auf die IT-Infrastruktur. IT Incident-Management im engeren Sinne muss sowohl organisatorische als auch rechtliche sowie technische Detailfragen berücksichtigen.

Die Risiken, dass Hacker einen Angriff erfolgreich zum Abschluss bringen, sind vielfältig und ausgesprochen hoch. Die Cyberkriminellen selbst arbeiten mittlerweile hochprofessionell. Der Mythos vom einsamen Kapuzenpulli-Täter im Keller vorm Rechner ist schon längst Geschichte. Die Hacker von heute verfügen über diverse Manipulationsmittel und Verbreitungswege, um Erpressungstrojaner, Viren & Co. gewinnbringend ins Netzwerk zu mogeln. Und nicht immer wird ein Cyberangriff sofort bemerkt, weil nicht alle Systemebenen unter Beobachtung sind.

Bevor wir Ihnen zeigen, was sie bei einem erfolgreichen Cyberangriff tun müssen, geben wir Ihnen ein paar Tipps, worauf Sie bei der Erstellung eines Notfallplans achten müssen:

- **Entwickeln Sie einen betrieblichen Notfallplan:** Erfassen Sie alle notwendigen Maßnahmen, die im Ernstfall greifen müssen. Am besten lassen Sie sich professionell von Experten beraten. Einen ersten Überblick finden Sie auch in Mustervorlagen.
- **Legen Sie einen IT-Sicherheits-beauftragten fest:** Bestimmen Sie einen Verantwortlichen im Unternehmen, der sich mit Sicherheitsfragen befasst. Seit der DSGVO gilt: Ab mehr als zehn Mitarbeitern müssen Sie einen Datenschutzbeauftragten einsetzen.
- **Checken Sie Ihren derzeitigen Notfallplan:** Besitzen Sie bereits einen Notfallplan, sollten Sie ihn von Experten überprüfen und durchführen lassen. Überprüfen Sie auch, ob Ihr Notfallplan für Laien verständlich ist.
- **Wappnen Sie Ihr Unternehmen für den Fall der Fälle:** Damit Sie wirklich wissen, ob der Plan funktioniert, müssen Sie ihn unbedingt im Vorfeld in der Praxis testen.

Eine gute Vorbereitung für die Erstellung eines Notfallplans ist alles. Denn im Fall der Fälle geht es vor allem darum, rasch zu reagieren und so die Attacke so schnell wie möglich zu unterbinden, die gespeicherten Daten zu schützen und auch den Normalbetrieb des Unternehmens schleunigst wiederherzustellen. So gilt es, verschiedene Sofortmaßnahmen zu definieren, etwa wenn die gesamte Office-Kommunikation zusammenbricht, Webseiten nicht mehr verfügbar sind oder gar die ganze Produktion nach einer Attacke zum Stillstand kommt. Nur den Stecker ziehen reicht hier nicht aus.

Cyberangriff: Was aber kann man im Krisenfall tun – 9 Tipps für den Notfallplan

Mit fortschreitender Zeit richten Cyberkriminelle immer mehr Schaden an, infiltrieren die IT-Architektur bis ins kleinste Element oder saugen massenhaft sensible Daten ab. IT-Verantwortliche haben daher die Aufgabe, das schädliche Treiben frühzeitig zu erkennen und rasch zu handeln. Nur so können sie die eintretenden Schäden minimieren und sogar einen Totalausfall des Gesamtsystems vermeiden. Neben den finanziellen Folgen müssen Unternehmen vor allem einen enormen Image- und Vertrauensverlust der Kunden befürchten.

Was also tun, wenn Kriminelle Unternehmensdaten gekapert haben und die Bürokommunikation außer Betrieb ist? Scheuen Sie sich nicht davor, externe Hilfe in Anspruch zu nehmen.

- IT-Fachhändler- und Systemhäuser haben viel Erfahrung mit Cyberangriffen und können schnell und gezielt helfen.
- Auch die Zentrale Ansprechstellen Cybercrime der Polizei (ZAC) stehen Ihnen mit ihren Spezialisten zur Seite (übrigens auch zur Prävention von Cyber-Angriffen).
- Fundierte Informationen bei einem IT-Sicherheitsvorfall und zur Gestaltung eines Notfallplans bietet auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) an.

Diverse Checklisten und Maßnahmenkataloge stehen kostenlos zur Verfügung. Insbesondere die Notfallkarte für „Verhalten bei IT-Notfällen" ist sehr zu empfehlen. Denn oftmals werden digitale Probleme frühzeitig erkannt, aber Mitarbeiter wissen selten, an wen sie sich zuerst wenden sollen. Hier hilft diese Karte weiter und beschleunigt die krisengerechte Kommunikation.

Wir haben für (betroffene) Unternehmen neun Tipps aus der Praxis parat, mit deren Hilfe Sie die Folgen einer Cyber-Attacke auf ein Minimum reduzieren können.

1. Einen kühlen Kopf bewahren und taktisch vorgehen

Wenn eine IT-Sicherheitssoftware Alarm schlägt, gilt es zunächst einmal, einen kühlen Kopf zu bewahren. Ein gelungener Cyberangriff kommt immer überraschend und ohne Voranmeldung. Schadsoftware kann sich mitunter wochenlang im Netzwerk verstecken, ohne bemerkt zu werden, wenn die IT nicht alle Systemebenen überwacht. Doch wenn es zu einem Vorfall kommt, gilt es, in kürzester Zeit die richtigen Entscheidungen zu treffen. Ohne einen Notfallplan mit festgelegten Sofortmaßnahmen kann Chaos quasi vorprogrammiert sein.

2. Das Ausmaß der Infektion ermitteln

Viele IT-Abteilungen von Betrieben, die Opfer einer Malwareattacke werden, vertrauen auf ihre Intuition statt auf gründliche Analysen, um die Folgen solcher Angriffe zu ermitteln. Natürlich ist es wichtig, umgehend darauf zu reagieren – aber nicht auf Basis von Vermutungen. Verfügt ein Unternehmen über ein funktionierendes IT-Notfallmanagement, kann die IT-Abteilung schnell die richtigen Antworten auf zentrale Fragen finden:

- Welche Systeme wurden infiziert?
- Auf welche Weise ist dies geschehen?
- Sind unternehmenskritische Datenabhandengekommen?
- Betrifft die Infektion nur einzelne Komponenten oder ein ganzes Subnetzwerk?
- Fielen Kundeninformationen und Mitarbeiterdaten in die Hände der Angreifer?

3. Den IT-Betrieb sicherstellen

Sind Unbefugten interne Informationen in die Hände gefallen, müssen zunächst die betroffenen Mitarbeiter und Kunden informiert werden. Werden IT-Systeme in starkem Maße von einem Angriff beeinträchtigt, sollten Reserve-Systeme und redundante Netzwerkverbindungen aktiviert werden. Denn der Geschäftsbetrieb darf nicht unter einem Cyberangriff leiden. Um das sicherzustellen, ist zudem ein Notfallplan erforderlich, der die Reaktionszeiten verkürzt.

Sie müssen sicherstellen, dass:

- sich aus der entdeckten Attacke keine weiteren Schäden ergeben können
- Sofortmaßnahmen unabhängig von übergeordneten Abteilungen oder der Chefetage eingeleitet werden können, damit keine Zeit verloren geht, um noch Zustimmungen im Krisenfall einzuholen.
- Zugangsdaten sofort geändert werden. Geklaute Passwörter, Logins und verseuchte E-Mail-Konten können auch künftig weitere Schäden verursachen. Ihr Notfallplan sollte also eine Strategie beinhalten, wie nach einem Hacker-Angriff mit firmeneigenen Zugangsdaten verfahren wird.
- auch Gäste-Zugänge, soweit vorhanden, deaktiviert werden und das Netzwerk offline geht. Gerade von nicht gemanagten Gästegeräten geht ein hohes Risiko aus, dass Schadcode auf das System gelangt.
- zudem keine E-Mails geöffnet, mobile Geräte weder im Firmennetz noch in anderen, z. B. Kundennetzen angemeldet werden, alle am Netzwerk angeschlossenen Speichermedien, wie USB-Sticks, externe Festplatten, Kameras etc., abgekoppelt und weder benutzt noch vom Arbeitsplatz entfernt werden.

4. Die Infektion eindämmen

Anschließend gilt es, die infizierten IT-Systeme zu isolieren. Um die Ausbreitung der Infektion im Netzwerk zu verhindern, kann die IT-Abteilung die Netzwerksegmente abkoppeln, in denen sich die befallenen Rechner befinden. Dadurch haben Angreifer keinen Zugang mehr zu diesen Systemen und können keine verwertbaren Daten „absaugen".

In jedem Fall sollte die IT-Abteilung versuchen, den verschlüsselten Datenverkehr zwischen den infizierten IT-Systemen im eigenen Netzwerk und den Rechnern der Angreifer zu decodieren. Auf diese Weise lässt sich feststellen, ob weitere Rechner im Netzwerk verseucht wurden und welche Firewall-Regeln erforderlich sind, um nicht autorisierte Zugriffe zu unterbinden. Solche Gegenmaßnahmen lassen sich erheblich schneller und effizienter umsetzen, wenn ein Unternehmen eine IT-Sicherheitslösung einsetzt, wie beispielsweise die neuen Business-Lösungen von ESET.

5. Beweise sichern

Damit nach einer erfolgreichen Attacke die Strafverfolgungsbehörden aktiv werden können, sollten unbedingt Beweise vom Vorfall gesichert werden. Eine umfassende Dokumentation hilft Ihnen ggf. auch, eine zuvor abgeschlossene Cyber-Versicherung tatsächlich in Anspruch nehmen zu können.

6. Die Infektion eliminieren und weitere Attacken verhindern

Zu den anspruchsvollsten Aufgaben zählt, die befallenen IT-Systeme von Schadsoftware zu säubern und weiteren Attacken über denselben Weg einen Riegel vorzuschieben. Ein bewährtes Mittel ist der Einsatz einer Anti-Viren- beziehungsweise Anti-Malware-Software, die IT-Systeme automatisch reinigt. Um weitere Angriffe derselben Art zu unterbinden, sollten die Sicherheitslöcher beseitigt werden, die diese Aktivitäten ermöglicht haben. Um ganz sicher zu gehen, empfiehlt es sich, die Datenpakete zu analysieren, die über das Netzwerk transportiert werden. Der Traffic sollte insbesondere auf Verkehrsmuster und Befehle hin untersucht werden, welche die Angreifer zuvor verwendet haben.

Weitere Sicherheitsvorkehrungen sind die Überprüfung der Firewall-Regeln und die Änderung der Passwörter, mit denen sich Mitarbeiter am Netzwerk anmelden. Es ist eine Überlegung wert, ob eine tiefer greifende Analyse des Cyberangriffs erfolgen soll. Denn in vielen Fällen sind einzelne Angriffe ein Bestandteil von „Advanced Persistent Attacks" (APT). Dies sind fortlaufende, komplexe und zielgerichtete Cyberattacken auf KMU oder deren Mitarbeiter. Wurde eine Verwaltung Ziel solcher ATPs, ist davon auszugehen, dass weitere Attacken folgen werden.

7. Juristisches regeln – Stichwort DSGVO

Nach einem Cyberangriff treten rechtliche Fragen auf den Plan, die Sie vorab klären sollten. Seit Einführung der DSGVO müssen bestimmte Vorfälle binnen einer Zeitfrist an Behörden gemeldet werden. Es gilt, vorab Informationspflichten mit der Rechtsabteilung zu regeln, damit Ihr Unternehmen rechtskonform bleibt und keine zusätzlichen Bußgelder im Nachgang zahlen muss.

8. Bei Ransomware-Angriffen nicht zahlen

Erpressersoftware ist ein beliebtes Angriffsmittel der Cyberkriminellen. Die Schadsoftware verschlüsselt die Daten der Opfer und die Hacker verlangen anschließend ein Lösegeld zur Freigabe der Daten. Zahlen Sie keinesfalls das geforderte Lösegeld – denn sie können nicht sicher sein, dass Sie Ihre Daten wiederbekommen. Darüber hinaus unterstützen Sie dieses „Finanzierungsmodell" der Cyberkriminellen und signalisieren Zahlungsbereitschaft, was Hacker als erneute „Einladung" verstehen.

9. Aus Cyberangriffen und Fehlern lernen

Wichtig ist, dass Unternehmen aus der Analyse von Angriffen die richtigen Schlüsse ziehen und entsprechende Vorkehrungen treffen. Jede Schwachstelle, die zuvor nicht bekannt war und beseitigt wurde, bietet letztlich die Chance, die Abwehrmaßnahmen am Rand (Perimeter) des Unternehmensnetzes zu verbessern und potenzielle Einfallstore zu schließen.

Entscheidend ist auch, dass der IT-Verantwortliche, alle Systemebenen genau im Blick hat. So lässt sich ein Cyberangriff frühzeitig erkennen und gibt den Eindringlingen keine Möglichkeit, sich in Bereichen einzunisten und das System auszukundschaften, bevor sie den eigentlichen Angriff starten.

Fünf extra Tipps für mehr Sicherheit

Mit diesen oben genannten Schritten sind Sie schon sehr gut auf den Krisenfall vorbereitet. Wir geben Ihnen noch fünf weitere Empfehlungen, die Ihnen helfen, Ihre Security im Unternehmen noch zu optimieren:

1. **Automatisieren Sie so viel wie möglich**

Im besten Falle kann der Notfallplan mithilfe von modernen Tools zu großen Teilen automatisiert werden. Alle Vorgänge, die von selbst abgearbeitet werden können, entlasten den Administrator. Solche Aktionen können etwa das automatische Abkapseln von betroffenen Endpoints sein, indem die Desktop-Firewalls jegliche Verbindungen bis auf die der Remote-Verwaltung kappen.

2. **Achten Sie auf Logging und Dokumentationen**

Wichtig ist außerdem, dass bei allen Aktionen, egal ob automatisch oder manuell, ein umfassendes Logging sowie Dokumentationen der manuellen Schritte erfolgen. Nur so lässt sich das Infektionsgeschehen im Nachhinein nachverfolgen und entsprechend der Notfallplan anpassen – was das Schließen von eventuellen Sicherheitslücken, aber auch das menschliche Verhalten angeht.

3. **Machen Sie regelmäßige Backups**

Was auch immer den Sicherheitsvorfall verursachte, entscheidend ist, dass Unternehmen die verlorengegangenen, unternehmenskritischen Daten so schnell wie möglich wiederherstellen können. Dies beginnt mit regelmäßigen Backups. Auch hier ist das automatische Sichern von Datenkopien eine gute Wahl, denn so wird die Konsistenz von Informationen gewährleistet. Darüber hinaus stellt man sicher, dass Mitarbeiter nicht vergessen, Backups zu machen. Die Sicherungskopien sollten auf mindestens zwei externen Medien vorgenommen werden, auch eine verschlüsselte Version eines Backups im Cloud-Speicher sollte in Erwägung gezogen werden (angesichts des Datenschutzes sollten Sie auf europäische Speicherorte setzen). Auch hier gilt: Backup- und Recovery-Systeme müssen regelmäßig getestet werden.

4. **Setzen Sie ein Endpoint Detection & Response (EDR) Tool ein**

Dank einem EDR Tool ist eine konstante und umfassende Überwachung aller Endpoint-Aktivitäten möglich. Dadurch werden verdächtige Prozesse eingehend analysiert und IT-Verantwortliche können frühzeitig auf Bedrohungen reagieren. Unternehmen steigern mit Einsatz einer EDR Technologie ihre Security um ein Vielfaches, vor allem wenn es um Zero-Day-Angriffe, Ransomware, zielgerichtete Attacken (Advanced Persistent Threats) oder auch Verstöße gegen die internen Unternehmensrichtlinien geht.

5. **Stellen Sie Ihren Notfallplan regelmäßig auf den Prüfstand**

IT-Notfallpläne, müssen – genauso wie Brandschutzübungen – regelmäßig getestet werden. Nichts ist fataler, als auf den Plan zu vertrauen, der am Ende gar nicht funktioniert.

Fazit

Wenn PCs, Server oder Mobilsysteme mit Schadsoftware verseucht werden, kann das eine ernst zu nehmende Gefahr für Organisationen darstellen. Vor allem dann, wenn den Angreifern interne Informationen in die Hände fallen. Aber solche Vorfälle führen den Verantwortlichen zwei wichtige Fakten vor Augen: Zum einen welche IT-Sicherheitsmaßnahmen optimiert werden müssen. Zum anderen, dass ein aktuelles Notfallsystem Schäden minimieren kann.

ÜBER ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihr Netzwerk mit Hilfe von Cloud-Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungsprodukte unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen.

Unsere XDR-Basis mit Endpoint Detection and Response Lösung, Frühwarnsysteme (bspw. Threat Intelligence) und dedizierte Services ergänzen das Angebot im Hinblick auf Forensik sowie den gezielten Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht nur allein auf Next-Gen-Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

ZUFRIEDENE KUNDEN

BVB 09 Champion Partner

Seit 2019 ein starkes Team
auf dem Feld und digital

Allianz Suisse

Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Secur|Ty made in EU
Trust Seal
www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel
„IT Security made in EU" verliehen

CERTIFIED ISO 9001:2015 COMPANY
CERTIFIED ISO 27001:2013 COMPANY

Unsere Lösungen sind nach
Qualitätsstandards zertifiziert

ESET IN ZAHLEN

110+ Mio.
Geschützte Nutzer weltweit

400k+
Geschützte Unternehmen

200+
Länder & Regionen

13
Forschungs- und Entwicklungszentren weltweit

welivesecurity by ESET