Leitfaden: **Was tun bei einem Cyberangriff?**

Wir arbeiten alle tagtäglich mit Computern, aber die wenigsten von uns sind Computerexperten und wissen, wie man in diesem Moment richtig vorgeht. Was Sie tun und was Sie im Gegenzug auf jeden Fall unterlassen sollten, erfahren Sie auf den folgenden Seiten.

perseus.
Cybersicherheit auf den Punkt

Es ist der Albtraum eines jeden Mitarbeiters: Sie arbeiten an einem Dokument, recherchieren im Internet oder gehen Ihre E-Mails durch und plötzlich "spinnt" der Rechner. Auf dem Bildschirm erscheint eine bedrohliche Nachricht: Ihr Computer warnt, er sei mit Schadsoftware infiziert. Programme öffnen und schließen sich scheinbar wie von Geisterhand oder das Gerät funktioniert gar nicht mehr. Der Monitor wird schwarz oder zeigt eine Nachricht von Cyberkriminellen an, die Ihnen mitteilen, dass alle Ihre Nutzerdaten durch eine Verschlüsselung in digitale Geiselhaft genommen wurden und die Kriminellen nun Lösegeld fordern. Oder sie haben angeblich vertrauliche Informationen über Sie gestohlen und drohen sie zu veröffentlichen. Und übrigens: Ihre Backups sind ebenfalls kompromittiert.

Vorbeugung statt Schadensbehebung

Wie diese Beispiele verdeutlichen, können Cyberangriffe sehr vielfältig sein. Manche sind eher lästig, andere können Ihr gesamtes System und alle Daten zerstören. Und wieder andere geben vor, gefährlich zu sein, werden es aber erst, wenn Sie unüberlegt auf die scheinbare Bedrohung reagieren.

Gegen die meisten Cybergefahren kann man sich mit relativ einfachen Mitteln im Vorfeld schützen. Die **wichtigsten Maßnahmen**, die jeder Computernutzer ergreifen sollte, sind hierbei:

1. Klicken Sie nach Möglichkeit nie auf **Links** oder **Anhänge in E-Mails**, insbesondere, wenn Sie den Absender nicht kennen. Besuchen Sie Webseiten im Zweifel direkt durch Eingabe der URL im Browser und fragen Sie (beispielsweise telefonisch) nach, ob Ihnen der Absender wirklich einen Anhang oder den Link geschickt hat, um zu verifizieren, ob es sich um einen Betrugsversuch handelt.

2. Öffnen Sie keine **Speichermedien** (USB-Sticks, DVDs, etc,) deren Herkunft Sie nicht kennen. Wenn Sie Dateien übertragen oder herunterladen, scannen Sie diese immer zunächst auf Schadsoftware.

3. Verwenden Sie unbedingt immer eine **aktuelle Antivirensoftware** und sorgen Sie dafür, dass diese immer mit den letzten Signatur-Updates versorgt wird.

4. Installieren Sie **Updates für** Ihr Betriebssystem und verwendete **Software** immer umgehend, sobald sie verfügbar sind. Verlassen Sie sich nicht darauf, dass sich jegliche Software auf Ihrem System automatisch auf dem neuesten Stand hält. Starten Sie Ihre Systeme umgehend neu, sobald dies aufgrund eines Updates gefordert sein sollte.

5. Aktivieren Sie die **Firewall** Ihres Computers.

6. Meiden Sie **öffentliche WLAN-Netzwerke**.

Richtig **Handeln** im Notfall

1. **Reagieren Sie umgehend**
   Niemand gibt gerne falschen Alarm. Und selbst wenn es kein falscher Alarm ist: was, wenn ich das Problem selbst verursacht habe? Trotzdem: es ist extrem wichtig, dass Sie mögliche Cyberangriffe umgehend Ihrem IT-Verantwortlichen melden, denn je mehr Zeit ohne Gegenmaßnahmen vergeht, umso mehr potentiellen Schaden können die Cyberkriminellen anrichten. Wer Ihr individueller IT-Verantwortlicher ist und wie Sie sie/ihn kontaktieren können, erfahren Sie weiter unten.

2. **Bewahren Sie Ruhe**
   Handeln ist wichtig, aber bitte besonnen und informiert. Viele Cyberangriffe richten überhaupt erst dadurch Schaden an, dass sie den Opfern Angst machen und diese dann unüberlegt handeln. Viele Phishing-Mails funktionieren so ("Laden Sie sofort diese Datei herunter, sonst wird Ihr Konto gelöscht…"). Bei anderen Angriffen erscheint eine Nachricht auf dem Monitor: man müsse dringend handeln, um Schadsoftware vom Rechner zu entfernen. Dafür müsse man Software herunterladen und installieren. Diese Software ist aber die eigentliche Bedrohung. Durch unüberlegtes Handeln, holen und installieren Sie die Schadsoftware so unter Umständen selbst auf Ihrem System. Die ursprüngliche Nachricht war harmlos.

3. **Dokumentieren Sie den Angriff**
   Statt unüberlegt zu handeln, sollten Sie in einem ersten Schritt die Situation dokumentieren. Fotografieren Sie mit dem Smartphone die Anzeige oder das ungewöhnliche Verhalten Ihres Computers. Und sammeln Sie so viel Informationen über den Vorfall, wie möglich und kontaktieren Sie dann Ihre IT-Abteilung bzw. den externen IT-Dienstleister Ihres Unternehmens und Ihren Vorgesetzten.

   Folgende Informationen sollten Sie sammeln:

   - Welches Gerät oder System ist betroffen? In den meisten Unternehmen erhält jedes Endgerät von der IT-Abteilung eine interne Gerätenummer, die meist auf dem Gerät aufgeklebt ist. So können die Verantwortlichen es eindeutig identifizieren. Falls das nicht vorhanden ist, sollten Sie wenigstens Hersteller und Modell des Geräts ermitteln.
   - Woran haben Sie gearbeitet, als das Problem auftrat? Welche Programme waren geöffnet, welche Dokumente?
   - Beschreiben Sie genau was passiert ist ("Der Bildschirm wurde blau", "das Bild flackerte", "das Gerät fing an zu piepen und der Lüfter lief plötzlich wie wild", etc.)
   - Wann ist es passiert?

4. **Schützen Sie Ihre Backups!**
   Falls Sie manuelle Backups Ihrer Daten machen, beispielsweise auf einer externen Festplatte, trennen Sie diese umgehend, nachdem ein Backup erstellt wurde (und nicht erst wenn eine Anomalie auf Ihrem System auftritt) um zu verhindern, dass sie ebenfalls mit Schadsoftware infiziert werden und so die Daten eventuell verloren gehen.

5. **Ausschalten oder nicht? - Kommt darauf an.**
   Diese Frage ist pauschal schwer zu beantworten. Wenn Sie das Gerät abschalten, oder die Netzwerkverbindung trennen, wenn Ihr Gerät für gewöhnlich dauerhaft angeschaltet bleibt, kann das die Cyberkriminellen alarmieren, dass ihre Aktivitäten entdeckt worden sind. Gleichzeitig erschwert es den IT-Experten die Analyse des Angriffs durch digitale Spurensuche. Auf der anderen Seite besteht die Gefahr, dass der Schaden größer wird, wenn die Täter weiterhin Zugriff auf Ihr Gerät haben und beispielsweise sensible Daten herunterladen können, oder Schadsoftware noch mehr Daten (z.B. über eingerichtete Netzlaufwerke) zerstört. Daher ist es im Zweifel immer besser, so schnell wie möglich einen Experten hinzuzuziehen, der Ihnen diese Entscheidung abnehmen kann.

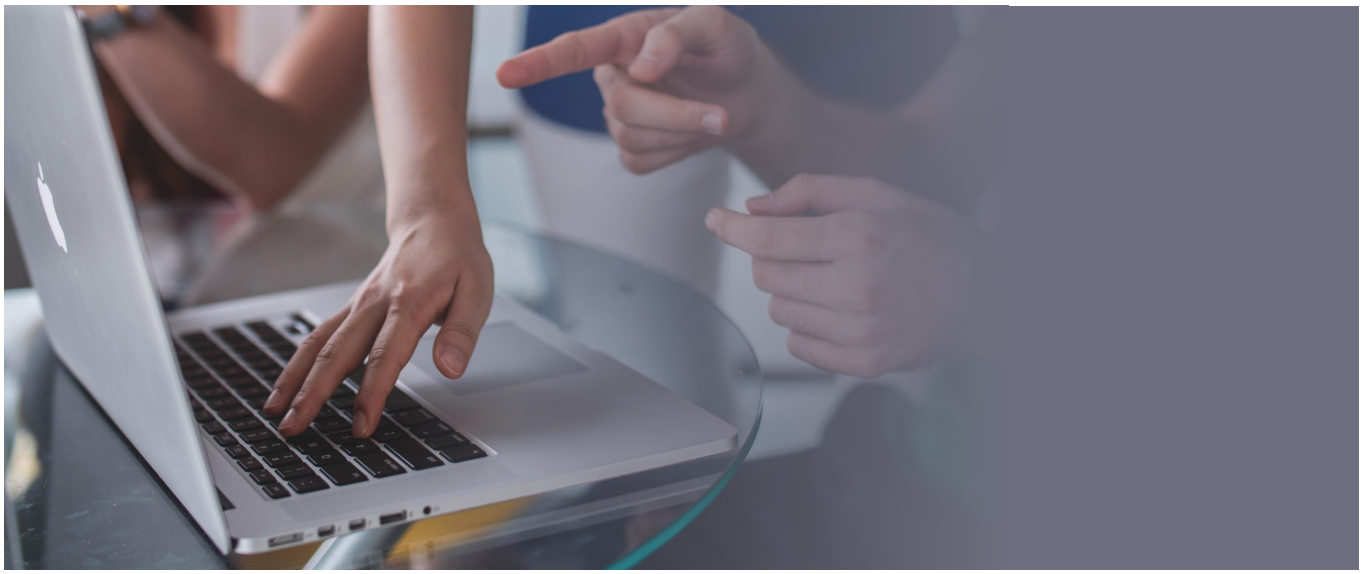
Was passiert, nachdem Sie einen **Cyberangriff** gemeldet haben?

Cyberangriff oder nicht?
Zunächst klären Cyberexperten, ob es sich wirklich um einen Cyberangriff gehandelt hat. Wenn der Computer ausfällt, kann ja auch einfach ein technischer Defekt vorliegen, oder der Anwender hat selbst einen Fehler gemacht, beispielsweise wichtige Daten versehentlich gelöscht. Egal was letztendlich der Grund für den Vorfall war, es ist wichtig, dass Sie ihn melden. Lieber einmal zu oft, als einmal zu wenig.

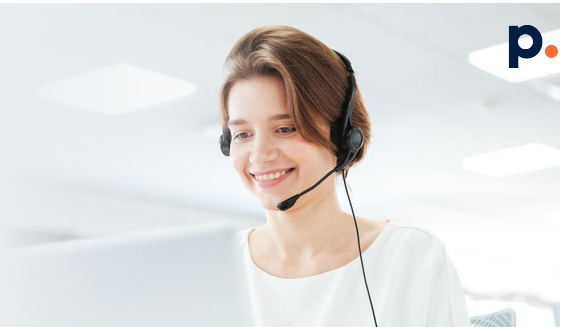
Digitale Spurensicherung und Analyse
Wenn sich herausstellt, dass es wirklich ein Angriff war, sichern die Cyberexperten zunächst Informationen wie Netzwerkprotokolle, Log-Dateien und Datenträger. Das ist quasi so wie die Spurensicherung, die einen Tatort in der realen Welt genau untersucht. Durch die anschließende Analyse lässt sich die Art des Angriffs und das Ausmaß des Vorfalls ermitteln. Mit diesen Informationen kann dann auch Anzeige bei der Polizei erstattet werden und gegebenenfalls eine Meldung bei der Datenschutzbehörde vorgenommen werden.

Wiederherstellung der Daten und Verbesserung des Systems
Jetzt, wo die Ursache des Angriffs bekannt ist, kann das System gezielt gereinigt, überwacht und gegen weitere Angriffe dieser Art geschützt werden. Auch zusätzliche Sicherheitsmaßnahmen können jetzt etabliert werden. So sollten z.B. neue Login-Daten und Passwörter für die Nutzer vergeben werden. Jetzt wäre auch ein guter Zeitpunkt, um eine 2-Faktor-Authentifizierung verpflichtend zu machen, falls das noch nicht geschehen war. Ebenfalls wichtig: jetzt wo das System wieder sicher ist, müssen eventuell verlorene oder beschädigte Daten wiederhergestellt werden.

Wenn all das erreicht wurde, sollten Sie wieder normal arbeiten können und sind auch noch besser gegen den nächsten Angriff gewappnet. In diesem Sinne: Bleiben Sie sicher!



Checkliste für **den Notfall:**



1. **Reagieren Sie umgehend**
2. **Bewahren Sie Ruhe**
3. **Arbeiten Sie nicht mehr an dem Gerät**
4. **Dokumentieren Sie den Angriff**
   - Welches Gerät oder System ist betroffen?
   - Woran haben Sie gearbeitet, als das Problem auftrat?
   - Welche Programme waren geöffnet, welche Dokumente?
   - Beschreiben Sie genau was passiert ist.
   - Wann ist es passiert?
5. **Schützen Sie Ihre Backups!**
6. **Kontaktieren Sie den zuständigen Cyberexperten**

Drucken Sie diese Karte bitte aus, ergänzen Sie die nötigen Informationen und hinterlegen Sie sie griffbereit an Ihrem Arbeitsplatz.

Ihr Kontakt im Fall eines Cyberangriffs:

Wenn Sie glauben, Opfer eines Cyberangriffs geworden zu sein, kontaktieren Sie bitte umgehend:

Name: .....

Position: .....

Telefon: .....

E-Mail: .....

(Senden Sie **auf keinen Fall** eine E-Mail von dem Computer, der vom Cyberangriff betroffen ist!)

Wir kümmern uns um Ihre **Cybersicherheit**, Sie sich um Ihre Geschäfte.

Perseus 360° Cybersicherheitspaket abschließen und Bußgelder, Betriebsunterbrechungen und Reputationsschäden vermeiden!

Unsere Angebote

Start

Individuell vorsorgen

Perfekt für die Einzelperson, die kostenlos und schnell die Grundlagen der Cybersicherheit und des Datenschutzes erlernen möchte, Online jederzeit und an jedem Ort.

Pro

Ganzheitlich schützen

Cybersicherheit als Komplettservice: Perfekt für kleine und mittlere Unternehmen, die eine einfache, günstige und umfassende Cybersicherheits- und Datenschutzlösung suchen.

Premium

Zusätzlich abgesichert

Perfekt für Unternehmen, die mit einer zusät- zlichen Kostenabsicherung Ihr Cyberrisiko minimieren wollen Cybersicherheit Komplettservice mit Kosten-Airbag.

Alle Funktionen	Start	Pro	Premium
Online-Sicherheitstraining	✓	✓	✓
24h/7 telefonische Notfallhilfe	✗	✓	✓
Simulierte Phishing-E-Mails	✗	✓	✓
Cybersicherheits-Führerschein	✗	✓	✓
Datenschutz-Führerschein	✗	✓	✓
IT-Sicherheitsprüfung	✗	✓	✓
Cybersicherheitsübersicht für Ihr Unternehmen	✗	✓	✓
Kundenservice Hotline	✓	✓	✓
Malware-Scanner	✗	✓	✓
Browser-Check	✓	✓	✓
Passwort-Generator	✓	✓	✓
Datensicherheits-Check	✗	✓	✓
Angriffsalarm	✗	✓	✓
Cyber-Schutzbrief			
IT-Forensik-Experten vor Ort	✗	✗	✓
Datenwiederherstellung und Entfernung der Schadsoftware	✗	✗	✓
Systemverbesserung nach Angriff (bis zu 10.000 €)	✗	✗	✓
Prüfung datenschutzrechtlicher Informationspflichten (bis zu 2.000 €)	✗	✗	✓

Über **Perseus**

Perseus bietet Unternehmen einen 360-Grad-Service für Cyber-Sicherheit und Datenschutz an. Ziel von Perseus ist die Etablierung einer langfristigen Sicherheitskultur zur Prävention, Abwehr und finanziellen Absicherung gegen Cyber-Kriminalität. Die Leistungen umfassen u.a. regelmäßige Phishing-Simulationstests, browserbasierte Mitarbeitertrainings, eine 24/7-Cyber-Notfallhilfe und eine intelligente Antivirensoftware.

Noch weitere Fragen?

Vereinbaren Sie einen unverbindlichen Beratungstermin mit unserem Kundenservice:

Hardenbergstr. 32, 10623 Berlin
Telefon: 030/95 999 80 80 (Mo - Fr 09:00-18:00 Uhr)
E-Mail: info@perseus.de

www.perseus.de

perseus.
Cybersicherheit auf den Punkt