perseus.
Cybersicherheit auf den Punkt

Bereiten Sie Ihr Team auf den Cyber-Notfall vor!

Unser Notfallplan soll Ihre Mitarbeiter optimal auf den Fall eines Cyberangriffs vorbereiten.

Er umfasst:

1. Tipps zu Maßnahmen, die im Vorfeld getroffen werden sollten, und
2. einen Leitfaden, wie sich die Mitarbeiter im Ernstfall verhalten sollten.

Bitte ergänzen Sie den Namen und die Telefonnummer des IT-Administrators auf der dritten Seite unter "Ihr IT-Administrator" und drucken Sie anschließend die zweite und dritte Seite des Dokuments aus.

Stellen Sie jedem Ihrer Mitarbeiter jeweils eine Version des Cyber-Notfallplans zur Verfügung.

Vergewissern Sie sich, dass Ihre Mitarbeiter den Cyber-Notfallplan gelesen und verstanden haben.

Beste Grüße aus Berlin,

Ihre Perseus Team

Perseus Technologies GmbH
Hardenbergstr. 32 / 10623 Berlin
030/95 999 80 80
support@perseus.de

perseus.
Cybersicherheit auf den Punkt

Cyber-Notfallplan – jetzt vorbereiten!

Wie erkenne ich einen Cyberangriff?

1. Veränderte Dateien oder Inhalte
Achten Sie auf plötzlich veränderte **Symbole, Datei-Endungen** oder **Datei-Inhalte**. Dies könnten Anzeichen eines Cyberangriffs sein.

2. Verdächtige Meldungen
Eine **Popup** Nachricht mit einer Zahlungsaufforderung ist ein sehr deutliches Zeichen für eine Cyberattacke. Des Weiteren können plötzlich auftretende **Systemfehlermeldungen** auf einen Virus hinweisen. Letzteres kann Ihr IT-Administrator für Sie prüfen.

3. "Automatisch" ausgelöste Aktionen
Sollten Dateien **abrupt verschwinden** oder **automatisiert E-Mails** über Ihren Zugang verschickt werden, ist das ein klares Zeichen. Ebenso eindeutig ist es, wenn Ihr Browser **eigenständig unseriöse Webseiten** aufruft.

Installieren Sie TeamViewer und notieren Sie sich Ihre ID und Ihr Passwort.

TeamViewer ist eine Software, mit der sich unsere IT-Sicherheitsexperten im Notfall per Fernsupport auf Ihren Rechner aufschalten und diesen untersuchen können.
Dafür benötigen wir lediglich Ihre TeamViewer **Identifikationsnummer** (ID) und Ihr automatisch erzeugtes **TeamViewer-Passwort**.
Bitte notieren Sie sich Ihre TeamViewer ID hier:

Wissen, wie Sie die Netzwerkverbindung trennen können.

Bei einem Angriff sollten Sie Ihren Rechner vom Internet und vom Firmennetzwerk trennen können. Vergewissern Sie sich, dass Sie die Funktionen bei Ihrem Rechner auch wirklich finden und bedienen können. Dazu können Sie am Rechner und auf Mobilgeräten den Empfang mobiler Daten ausschalten:

- WLAN
- mobiles Netz
- Kabelverbindung mit dem Firmennetz

Notieren Sie Sich Ihre Daten.

Benutzername:

Rechnerkennung:

Erstellen Sie regelmäßige Backups Ihrer Daten.

Programme lassen sich leicht neu installieren, aber Ihre Daten können bei einem Cyberangriff unwiederbringlich verloren gehen.
Machen Sie unbedingt **regelmäßige Backups** Ihrer Dateien oder verwenden Sie **Cloud- oder Netzwerkspeicher**, die in der Regel automatisch Sicherheitskopien anfertigen und somit selbst gegen die meisten Verschlüsselungsangriffe genug Sicherheit bieten.

Notfallplan ausdrucken und griffbereit legen.

Der "Cyber-Notfallplan: So verhalten Sie sich richtig." sollte in **ausgedruckter** Form immer **griffbereit** liegen, so dass Sie bei einem evtl. Ausfall Ihres Rechners durch eine Cyberattacke darauf zugreifen können.

perseus.
Cybersicherheit auf den Punkt

Richtiges Verhalten bei einem Cybersicherheits-Zwischenfall

Bewahren Sie Ruhe.	Nicht immer muss hinter verdächtigen Aktivitäten auf Ihrem Computer ein Cyberangriff stecken. Selbst wenn Sie angegriffen wurden, gilt: Ruhe bewahren, keine Kurzschlussreaktionen, dem Notfallplan folgen und umgehend Hilfe beim IT-Verantwortlichen suchen. **Arbeiten Sie auf keinen Fall weiter auf dem betroffenen Gerät!**
Informieren Sie Ihren IT-Administrator oder die IT Abteilung.	Suchen Sie umgehend Hilfe bei Ihrem IT-Verantwortlichen. **Name:** _____ **Telefonnummer:** _____ Ihr erster Ansprechpartner ist IMMER der IT-Administrator! Nur Ihr IT-Administrator kann entscheiden, ob Sie eine Cyber-Notfallhilfe in Anspruch nehmen müssen.
Trennen Sie die Netzwerkverbindung.	Vielleicht versendet Ihr Rechner gerade geheime Firmendaten oder wird von einem Hacker heimlich im Hintergrund ferngesteuert. Durch die Trennung der Netzverbindung **schützen Sie Ihre Firmengeheimnisse** und verhindern eventuell, dass Ihr Rechner noch andere Rechner Ihrem Netzwerk infizieren kann.
Lassen Sie Ihren Computer angeschaltet.	Nachdem Sie die Internet- und Netzwerkverbindung getrennt haben, ist es in der Regel empfehlenswert, Ihren Rechner angeschaltet zu lassen, damit **Cybersicherheit-Experten** den Vorfall korrekt analysieren können.
Wenn Sie erpresst werden, folgen Sie auf keinen Fall den Anweisungen, sondern wenden Sie sich immer an Ihren IT-Verantwortlichen.	Eigentlich selbstverständlich: Wer andere erpresst, ist **auf keinen Fall vertrauenswürdig.** Wer an einen Cyber-Erpresser Geld überweist, bekommt deshalb noch lange nicht seine Daten zurück – egal was der Verbrecher vorab verspricht.
Warnen Sie Ihr Team.	Sollten Sie die Befürchtung haben, dass Kollegen ebenfalls Opfer des Angriffs werden könnten (z.B. wenn eine Phishing-E-Mail der Auslöser war,) dann warnen Sie Ihre Kollegen oder bitten einen Verantwortlichen (Gesch.ftsführer, IT-Administrator) darum.
Dokumentieren Sie den Vorfall.	Wenn möglich, **fotografieren** Sie Ihren Bildschirminhalt mit einem anderen Gerät (z.B. Handy). Alternativ können Sie den Vorfall selbstverständlich auch **schriftlich** festhalten.