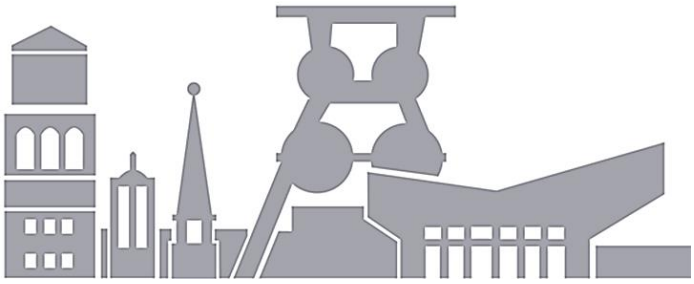
POLIZEI
Nordrhein-Westfalen
Essen



…gemeinsam erfolgreich - für Sicherheit in Essen und Mülheim

Cybercrime

Präventionsmaßnahmen für kleine und mittelständische Unternehmen

---

Maßnahmen zur Vorbeugung gegen IT-Angriffe

IT-Sicherheit in Firmen ist Chefsache!

Ist ein Angriff erst einmal erfolgreich durchgeführt, gibt es keinerlei Gegenmaßnahmen außer einer Schadenbegrenzung mehr. Alle Maßnahmen müssen daher bereits im Vorfeld erfolgen, damit es gar nicht erst zu einem erfolgreichen Angriff kommt. Daher gilt grundsätzlich die Regel:

Cybersicherheit ist Chefsache!

Nur Geschäftsleitung oder Inhaber*in der Firma haben genug Einfluss, um sowohl planerisch, wie auch finanziell Entscheidungen zu treffen, die geeignet sind, die IT-Sicherheit des Unternehmens sicherzustellen. Das Delegieren dieser wichtigen Aufgabe an untergeordnete Gremien gefährdet mit großer Sicherheit den Erfolg der Absicherung!

Dabei muss es sich nicht - nur - um finanzielle Investitionen handeln. Es gibt zahlreiche Maßnahmen die - vor allem in Kombination - die Cybersicherheit des Unternehmens verbessern.

Nutzerberechtigungen festlegen

Das Prinzip „Jeder darf alles“ ist in vielen Firmen unterschiedlicher Größe noch immer IT-Alltag. Zu einer sicheren IT-Umgebung gehören Nutzungskonzepte, die alle Mitarbeitenden erfassen und ihnen sowohl Handlungsbereiche als auch innerhalb ihrer Handlungsbereiche auf die jeweilige Tätigkeit abgestimmte Nutzungsberechtigungen zuordnen. Die Zugriffsrechte sind dabei an Nutzerkonten zu koppeln, denen die Zugriffsberechtigungen erteilt werden. Eine Anmeldung mit persönlichen Zugangsdaten ist dabei einzurichten.

Einschränkungen des Zugriffs können dabei sinnvoll auf unterschiedlichen Ebenen und mit verschiedenen Zielrichtungen festgelegt werden. Neben der reinen Zugriffsmöglichkeit auf Informationen, Daten und Dateien der Firma sind beispielsweise auch Beschränkungen im Hinblick auf Nutzungszeit oder auch Infrastruktur (Drucker, Endgeräte etc.) denkbar.

Backup- und Recoveryplan erstellen

Die Datensicherung darf nicht willkürlich erfolgen. Das Backup aller Firmendaten muss automatisiert einem konkret festgelegten Sicherungsplan folgen.

Dabei ist auf folgende Faktoren größter Wert zu legen:

- Das Backup hat automatisch zu erfolgen
    - Nur eine Sicherung die automatisiert ist, wird auch durchgeführt. Eine manuelle Sicherung durch Mitarbeitende unterliegt prinzipbedingt immer dem Faktor Mensch. Beim Erstellen des Datensicherungskonzeptes müssen die Kriterien im Hinblick auf Häufigkeit, Umfang und dergleichen konkret festgelegt werden.
- Es muss mindestens ein Offline-Backup vorliegen
    - Alle gesicherten Dateien müssen sich neben den Ablageorten im Firmen-netzwerk mindestens auf einem Datenträger befinden, der keinen Zugang zum Firmennetz hat, von diesem also tatsächlich *physisch* getrennt ist.
- Brandschutz
    - Die Sicherung der Daten muss sich in einer gesonderten Brandzone befinden. Im Falle eines Feuerschadens müssen gesicherte Daten vor diesem Brand sicher sein.
- Das Backup muss geprüft werden
    - In regelmäßigen Abständen muss eine Funktionsprüfung des Backups erfolgen. Dabei werden alle gesicherten Dateien in einem Desaster-Recovery zurückkopiert. Erst wenn sichergestellt ist, dass die wiederhergestellten Daten und Dateien vollständig funktionieren, ist eine Datensicherung erfolgreich und sicher.
- Zuständigkeiten sicherstellen
    - Es muss mindestens eine Person bestimmt werden, welche die Aufgaben von Überwachung, Kontrolle und Verwaltung der Datensicherung verantwortlich übertragen wird. Eine Berichtspflicht in Richtung Geschäftsleitung ist dabei zwingend erforderlich.

Aktualisierung von IT-Systemen

Die Aktualität sowohl aller eingesetzten Softwareprodukte als auch verwendeter Endgeräte ist in einem Konzept sicherzustellen. Dabei müssen nicht unbedingt immer die neuesten Gerätegenerationen oder Programme verwendet werden, alle müssen jedoch im Rahmen von Sicherheits- und Funktionsupdates auf dem aktuellen Stand gehalten werden.

Diese Aktualisierung muss zwingend zeitnah und regelmäßig durchgeführt werden. Dabei ist besonderes Augenmerk darauf zu legen, ob eingesetzte Software seitens des Herstellers noch mit Aktualisierungen versehen wird. Alte Windows-Betriebssysteme (beispielsweise Windows XP oder Windows 7) werden von Microsoft nicht mehr mit Sicherheitsupdates versehen und sind daher *bedingungslos* (!) gegen aktuellere Versionen auszutauschen.

Automatische Gerätesperrungen

Aktuell nicht genutzte Endgeräte sind so einzurichten, dass nach einer festgelegten Zeit der Inaktivität das Gerät automatisch für die Nutzung gesperrt wird. Eine weitere Nutzung darf nur durch Anmeldung mit einer verwendeten Zugangskennung möglich sein.

Nutzung von Firewalls und Antiviren-Software

Auf Serversystemen muss eine Firewall eingerichtet werden, die Fremdzugriffe von außen überwacht und nach einem festzulegenden Regelkonzept zulässt oder unterbindet. Auf allen Endgeräten muss sich eine Antivirensoftware befinden, die stets auf dem aktuellen Stand gehalten wird.

Netzwerk-Segmentierung vornehmen

Ein Firmennetzwerk muss in Segmente unterteilt sein, die einen erfolgreichen Angriff in einem Segment nicht auf das gesamte Firmennetzwerk übergreifen lässt. Beispielsweise ist eine Netzwerktrennung von Abteilungen oder auch Liegenschaften verschiedener Standorte möglich.

Insbesondere sensible Bereiche, wie beispielsweise Backupsysteme, sind dabei mit besonderer Sorgfalt in geeigneter Weise vom Nutzungsnetz zu trennen. Der erfolgreiche Angriff auf das Firmennetzwerk darf in keiner Weise bestehende Backupsysteme erreichen.

Sperre entlassener Mitarbeitenden

Erfolgen Kündigungen von Arbeitsverhältnissen Mitarbeitender ist grundsätzlich - jedoch insbesondere im Konfliktfall - vor der Information der betreffenden Person über die Kündigung zunächst deren Zugriff auf alle Netzwerkressourcen und IT-Endgeräte der Firma zu unterbinden. Ein Zugriff unmittelbar nach der Kündigung darf nicht mehr möglich sein.

Schulung und Sensibilisierung aller Mitarbeitenden

Eine der größten Bedrohungen der IT-Sicherheit einer Firma ist der Faktor Mensch. Durch Manipulation von Mitarbeitenden erlangen Angreifer mit nur geringem Aufwand Zugriff auf die IT-Infrastruktur. Dabei werden Unkenntnis und Unachtsamkeit der Mitarbeitenden ausgenutzt, hier einige Beispiele:

- Social Engineering

  Solche Angriffe konzentrieren sich nicht auf ein System, sondern auf eine Person innerhalb der Firma. Durch gefühlsbasierte soziale Verhaltensweisen wie Angst, Gier oder Mitgefühl soll diese dazu gebracht werden, gewollt oder ungewollt, zumindest Hinweise auf Informationen etwa zu einem Login zu geben oder sonstige Daten und Informationen preiszugeben, die für kriminelle Handlungen genutzt werden können.

  Dabei sind die Vorgehensweisen keineswegs nur virtuell in elektronischer Form. Beispielsweise wird ein präparierter USB-Stick im Raucherbereich einer Firma ausgelegt und auf die Neugierde eines Mitarbeitenden gesetzt, diesen Stick in einen Firmenrechner einzustecken, um zu sehen, was sich darauf befindet.

- CEO - Fraud

  Beim CEO-Fraud oder auch „Fake President“ werden Angestellte einer Firma durch eine Nachricht, die scheinbar von einer Führungsperson kommt, zu einem Handeln oder Unterlassen bewegt. Das kann beispielsweise die sofortige Begleichung einer ebenfalls gefälschten Rechnung sein oder auch der Zugang einer fremden Person zu einem geschützten Bereich.

  In der Regel werden E-Mails mit einem gefälschten Absender generiert, deren Aussehen und textlicher Inhalt derjenigen der Firma entsprechen. Zumeist werden bereits im Vorfeld Informationen über die Firma eingeholt, um handelnde Personen zu identifizieren oder Betriebsabläufe und Zuständigkeiten kennen zu lernen.

- Phishing

  Phishing-Angriffe gegen Unternehmen zielen insbesondere darauf ab, an sensible Unternehmensdaten, z.B. Zugangsdaten, Passwörter, Daten von Bankkonten oder Kreditkartendaten, zu gelangen.

  Dazu werden häufig manipulierte Webseiten oder gefälschte E-Mails eingesetzt, um Mitarbeitende so zu täuschen, dass sie diese preisgeben. Die Kenntnis solcher Daten eröffnet den Tätern viele andere Angriffsmöglichkeiten, z.B. Manipulation und Umleitung von Transaktionsvorgängen oder Identitätsdiebstahl zur Täuschung Dritter.

Durch *regelmäßige* Schulungsmaßnahmen sind alle Mitarbeitenden zu sensibilisieren und zu steter Wachsamkeit anzuhalten. Die Schulung ist durch geeignetes internes Personal oder auch durch externe Dienstleister durchzuführen.

Der Ausfall an Arbeitszeit durch Schulungsmaßnahmen ist im Vergleich zu den umfangreichen Folgen eines erfolgreichen Angriffs auf die IT-Infrastruktur der Firma geradezu marginal.

Kennwortsicherheit

Ausreichende Kennwortsicherheit ist durch geeignete Maßnahmen, wie Schulungen oder auch technische Beschränkungen in Benutzerkonten sicherzustellen.

In besonders sensiblen Bereichen ist der Einsatz einer Zwei-Faktor Authentifizierung sinnvoll. Dabei erfolgt ein Zugriff durch verwendete Zugangsdaten erst nach Autorisierung durch ein weiteres Gerät. Beispielsweise folgt eine Anmeldung erst nach Eingabe eines Codes, der auf ein Firmenhandy gesendet wird.

Folgen eines erfolgreichen IT-Angriffs

Die Folgen sind zahlreich und vielfältig, hier einige Beispiele:

- Finanzieller Schaden

  Durch Umleitung von Zahlungen, Fremdzugriff auf Bankkonten oder auch durch Lösegeldzahlungen entstehen finanzielle Schäden, die nicht nur kleine und mittelständige Unternehmen an den Rand der Insolvenz bringen können.

- Rufschädigung

  Der Ruf einer Firma ist ihr Kapital. In der heutigen vernetzten Welt ist die allgemein erhältliche Information über die Unzuverlässigkeit einer Firma gleichbedeutend mit einem massiven Umsatzverlust. Wer einem Unternehmen misstraut, weil es erfolgreich angegriffen wurde, wird anschließend z. B. die eigenen Kreditkartendaten nicht mehr verwenden wollen.

- Produktionsausfall

  IT-gestützte Steuerungssysteme steuern heutzutage große Produktionsprozesse. Durch Verschlüsselung unbrauchbare IT-Systeme führen schnell zu einer Handlungsunfähigkeit des Unternehmens.

- Identitätsverlust

  Werden firmeneigene Kommunikationsmedien wie Mailadressen oder auch Social Media Konten (Facebook, Instagram etc.) von Angreifenden übernommen, können Nachrichten scheinbar im Namen der Firma herausgegeben werden, die das Unternehmen diskreditieren oder als Geschäftspartner ausschließen.

- Informationsverlust

  Der Verlust von Kundendaten, Terminen, Steuerunterlagen oder auch Firmengeheimnissen kann zu Handlungsunfähigkeit oder materiellem Schaden und damit zu einer nachhaltigen Schädigung des Unternehmens führen.

Dies sind nur einige wenige Folgen eines erfolgreichen Cyberangriffs, wobei diese Folgen nicht nur einzeln auftreten, sondern durchaus kombiniert vorkommen. So führt eine Netzwerkverschlüsselung gleichermaßen zu Produktionsausfall, Rufschädigung und finanziellem Schaden. Die Kombination verschiedener schädlicher Folgen ist dabei eher die Regel als die Ausnahme.

Worst Case Szenario - Checkliste
Handeln bei einem erfolgreichen Angriff

- Sofortige **physische** Trennung aller Komponenten vom Netzwerk.
    - Phsisch meint dabei konkret das Abziehen von Netzwerkkabeln.

- Zahlen Sie **kein Lösegeld**!
    - Sie können keinesfalls sicher sein, im Gegenzug erwartete Dateien oder Informationen zu erhalten - Verbrechern kann man nicht trauen. Darüber hinaus werden die Täter durch Zahlungen zu weiteren Angriffen ermutigt.

- Ziehen Sie **sofort** die **Polizei** hinzu.
    - Erstatten Sie Anzeige und wenden Sie sich dabei möglichst schnell an die Polizei - hier ist Geschwindigkeit gefragt, um Spuren sicherzustellen, die möglicherweise bereits nach kurzer Zeit nicht mehr vorhanden sind.

- Warten Sie mit dem Zurücksetzen der Endgeräte auf die Polizei.
    - Beachten Sie den Rat der erfahrenen IT-Forensiker, die Sie mit Ratschlägen bei der Erneuerung Ihrer IT-Infrastuktur unterstützen. Löschen Sie nicht bereits vor Eintreffen der Polizei Ihre Systeme!

- Kontrollieren Sie Ihr Backup.
    - Nun wird sich beweisen, ob Ihre Datensicherungsstrategie erfolgreich ist. Nachdem Ihre Systeme neu aufgesetzt sind, erfolgt das Desaster-Recovery (das Zurückkopieren) Ihres Datenbestandes.

- Ändern Sie die Zugangsdaten.
    - Nach einem erfolgreichen Angriff sind Zugangsdaten und Kennwörter kompronmittiert und müssen geändert werden.