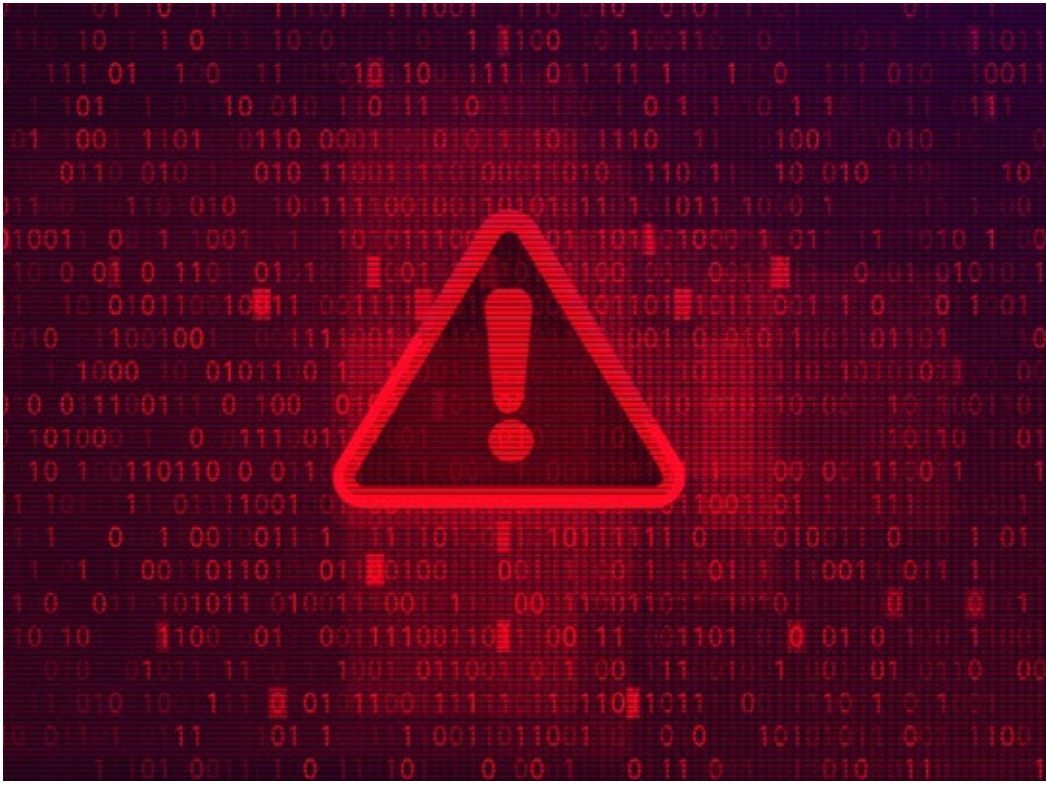
Ihr Leitfaden für sicheren Malware-Schutz



CYBERXPERTS

Inhaltsverzeichnis

Wer sind wir eigentlich und warum?

Liebe Leserin, lieber Leser,

Kompliment, dass Sie sich zum Thema Phishing und Awareness-Kampagnen informieren. Damit haben Sie einen wichtigen Schritt gemacht, Ihr Unternehmen vor Cyber-Angriffen zu schützen.

Warum das so dringlich ist, zeigen alarmierende Zahlen wie diese:

- Die schiere Anzahl an Phishing-Mails stieg im letzten Jahr um unglaubliche 29 % an.[1]
- Der Schaden durch Ransomware ist allein in Deutschland auf 24,3 Mrd. Euro angestiegen.[1]
- 45 % der Vorstände geben Cyber-Angriffe als das Hauptgeschäftsrisiko für ihr Unternehmen an.[2]
- Bei fast 9 von 10 Unternehmen in Deutschland haben Angriffe im letzten Jahr zu einem Schaden geführt.[3]
- Die Schäden für die Unternehmen stiegen auf 223,5 Mrd. Euro.[3]

Zur Versinnbildlichung der Größenordnung: 223,5 Milliarden Euro ist vergleichbar mit dem Jahres-Umsatz der gesamten Maschinenbau-Industrie in Deutschland.[4]

1 Bitkom e.V., Wirtschaftsschutzbericht 2021, 05.08.2022

2 KPMG, Ist Cybersecurity Chefsache?, 05.07.2022, abrufbar unter: https://hub.kpmg.de/ist-cyber-security-chefsache

3 Bitkom e.V., Wirtschaftsschutzbericht 2021, 05.08.2022

4 Bundesministerium für Wirtschaft und Klimaschutz, Maschinen und Anlagebau, 08.07.2022, abrufbar unter: https://www.bmwk.de/Redaktion/DE/Artikel/Branchenfokus/Industrie/branchenfokus-maschinen-und-anlagenbau.html

Wir finden: Es reicht!

Unternehmen können sich schützen – sie müssen nur wissen, wie!

Deshalb haben wir im Jahr 2022 das Security-Awareness-Plattform CyberXperts auf den Markt gebracht. Unternehmen erstellen mit CyberXperts:

- simulierte Phishing-Kampagnen,
- komplette Trainings für Mitarbeiter zur Prävention und
- einen intuitiven 360°-Check zur Einschätzung ihres Risikoprofils.

Mit CyberXperts erreichen Unternehmen eine Rundum-Sensibilisierung der Mitarbeiter für Cyber-Angriffe jeder Art.

Auch wenn CyberXperts als Produkt und Marke neu auf dem Markt ist: Das Team hinter CyberXperts ist es nicht.

Seit über 15 Jahren veröffentlichen wir Fachinformationen zum Thema Datenschutz und Datensicherheit im renommierten Fachverlag Privacy-Xperts aus Bonn. So verfügen wir über ein breites Netzwerk an Experten, die ihr gesamtes Wissen und ihre Erfahrung für den Start von Cyber-Xperts versammelt haben.

Und tatsächlich – das Feedback der Ersttester aus der Fachwelt ist überwältigend (Namen aus Datenschutzgründen geändert):

> *„Die Plattform ist schön einfach und verständlich gestaltet. Wir haben nun schon mehrere Lösungen ausprobiert, aber wir sind mit keiner zurechtgekommen. Bei cyberyxperts.de konnte ich direkt starten und bekam eine fertige Awareness-Kampagne für meine Mitarbeiter. Mir gefällt es gut, dass ich das Experten-Wissen gut aufbereitet erhalte. Endlich verstehe ich, was ich machen soll! Durch die automatische Dokumentation spare ich mir Zeit, da ich es nicht mehr über Excel machen muss."*
>
> Frau Schmitt, öffentliche Verwaltung

> *„Die Zeit ist reif für eine Lösung wie CyberXperts. Die Bedrohungslage ist so massiv gewachsen, dass kein Unternehmen um eine professionelle Unterstützung herumkommt."*
>
> Herr Scholl, Maschinenbau

„Das Portal ist wirklich nah am Bedarf der klein- und mittelständischen Unternehmen in Deutschland entwickelt. Gut gemacht!“

Herr Weber, Handel

„Auch wenn Unternehmen glauben, für Hacker uninteressant zu sein. Jedes – ich betone: JEDES (!) Unternehmen ist inzwischen Zielscheibe, z. B. für Ransomware. Ihr Produkt ist deshalb ein Must-have für alle.“

Herr Sauer, Lebensmittelindustrie

„Ich kenne ja einige Software-Anbieter für Cybercrime-Abwehr. Ihre Lösung gefällt mir sehr gut, insbesondere dass sie so intuitiv zu bedienen ist.“

Frau Stahl, IT-Branche

Wir laden Sie ein: Informieren Sie sich doch auch einmal kostenlos und unverbindlich zu Ihren Möglichkeiten mit CyberXperts. Klicken Sie hier, um Ihr Gratis-Strategie-Beratungsgespräch zu vereinbaren.

Wir freuen uns auf Sie!

Ihr Team von CyberXperts

Andreas Hessel
Chief Information Security Officer

Naomi Meier
Senior Sales Managerin

Executive Summary: So böse und schädlich ist Malware … und die Bedrohung wächst immer weiter an!

Die Folgen durch Malware sind enorm. Nicht umsonst geben 45% der Vorstände eine Cyberattacke als das TOP-Risiko für Ihren Konzern an.[5]

Betroffene Unternehmen erleiden **nicht nur finanzielle Schäden, sondern auch Reputationsverlust.** Das Ausmaß der Schäden hängt auch von der Malware-Art ab, wie schnell diese identifiziert wird und welche Daten und Zugänge auf den infizierten Endgeräten liegen.

Typische Schäden sind:

- Fehlfunktionen oder Verlangsamung des infizierten Geräts
- Datenverlust (z. B. wenn die Malware Daten löscht oder sperrt)

5 KPMG, Ist Cybersecurity Chefsache?, 05.07.2022, abrufbar unter: https://hub.kpmg.de/ist-cyber-security-chefsache.

- Diebstahl von Daten durch den Angreifer
- Hardware-Fehler
- Produktionsausfälle durch Fehler in der Software oder Verschlüsselung der Daten
- Erpressung durch Ransomware
- Reputationsverlust
- Kosten für die Schadensbeseitigung

Die weltweiten Schäden durch Cyberangriffe werden 2021 auf sechs Billionen Dollar geschätzt. Laut Experten kann die Summe bis 2025 auf 10,5 Billionen Dollar steigen. Insbesondere der Mittelstand sei betroffen, da hier oft nicht die ausreichende Infrastruktur zum Abschließen einer Cyberversicherung vorliegt und das eigene Risiko für Angriffe als gering eingeschätzt wird.[6]

Allein die Anzahl an Schadprogramm-Varianten sind 2021 im Vergleich zum Vorjahr um 22% gestiegen[7]

Eines der häufigsten Einfallstore für die Diebe, um Malware in Systemen zu platzieren, ist „Phishing".

Phishing ist oft der Startpunkt für schlimme Angriffe auf Unternehmensdaten und personenbezogene Informationen von beispielsweise Beschäftigten und Kunden.

Und so funktioniert Phishing:

Sie erhalten eine täuschend echt aussehende E-Mail angeblich von Behörden, Banken, Software-Programmen oder Online-Shops. Diese ist so formuliert und gestaltet, dass Sie sich unter Druck gesetzt fühlen. Um Schaden oder Ärger zu vermeiden, sollen Sie eine Datei öffnen oder sich auf einer gefälschten Website mit Ihren Benutzerdaten anmelden. Etwa eine Rechnung, einen Antrag oder einen Fragebogen. Öffnen Sie den Anhang, wird Ransomware installiert. Diese bösartige Software (Malware) verschlüsselt im Hintergrund alle erreichbaren Daten. Nur gegen Zahlung

6 Tagesschau, Cyberangriffe größte Gefahr für Firmen, 22.09.2022, abrufbar unter: https://www.tagesschau.de/wirtschaft/unternehmen/cyberattacken-unternehmen-risiken-101.html.

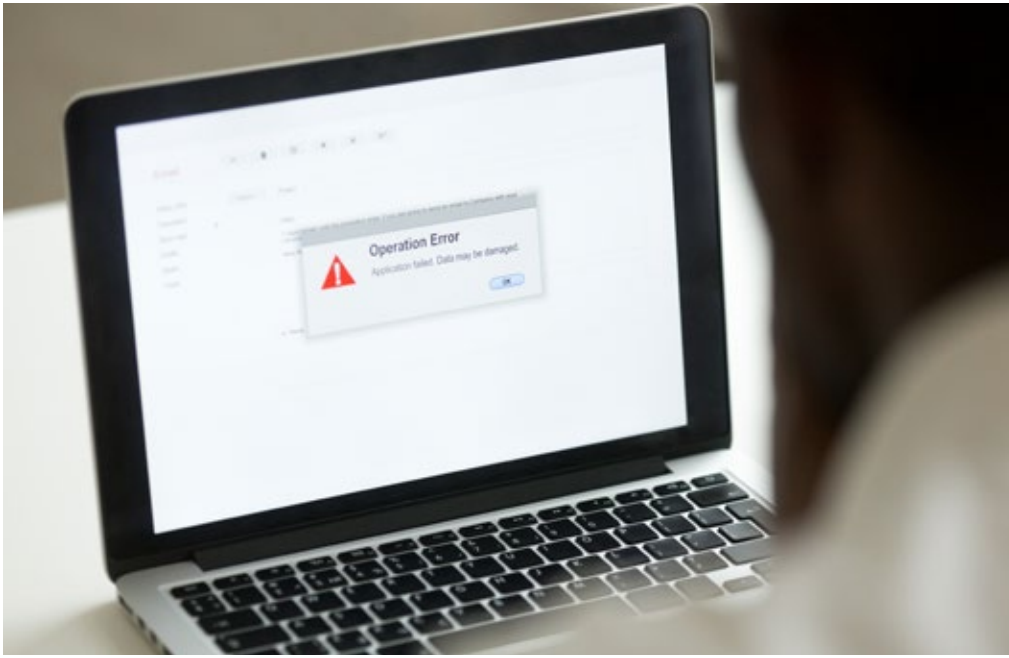
7 BSI, Die Lage der IT-Sicherheit in Deutschland 2021, 06.07.2021, abrufbar unter: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

eines „Lösegelds“ soll das Unternehmen die Informationen zur Entschlüsselung seiner Daten erhalten.

Phishing war 2021 Haupteinfallstor für Kriminelle um Login-Daten, Banking-Informationen zu erhaschen oder Malware zu platzieren. Die erbeuteten Daten werden dann im Darknet verkauft und gehandelt.[8]

Die Angriffe steigen in den letzten Jahren rasant an und sind spätestens seit der Corona-Pandemie eine außerordentliche Bedrohung für Unternehmen.

Durch die Pandemie nahm die Nutzung von digitalen Angeboten noch einmal stark zu – sowohl im privaten Bereich als auch beruflich. Cyberkriminelle nutzten diese Verlagerung in die digitale Welt in Verbindung mit den aufkommenden Ängsten und Verunsicherungen der Menschen aus, um vermehrt Angriffe zu streuen.[9]



8 BKA, Bundeslagebericht Cybercrime 2021.

9 BKA, Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie, 12.07.2022, Abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeSonderauswertungCorona2019.html.

Malware, Trojaner, Ransomware … was ist das eigentlich?

Malware (auf Deutsch: Schadsoftware) bezeichnet **Software, die in böser Absicht Schaden an einem System anrichtet.** Schadsoftware ist ein Überbegriff und lässt sich in verschiedene Arten unterteilen, z. B. Trojaner, Viren, Würmer etc.

Viren: Ein Virus ist ein schädlicher Code, der Dateien infiziert und sich dadurch selbst vermehrt.

Trojaner: Ein Trojaner ist eine Software, die sich selbst tarnt und dadurch in Systeme eindringen kann. Den Namen verdankt sie daher auch dem Trojanischen Pferd aus der griechischen Mythologie. Klassischerweise wird ein Trojaner heruntergeladen, da das Opfer denkt, dass es sich um eine harmlose Datei handelt.

Spyware: Die Art von Malware hat zum Ziel, den Nutzer gezielt auszuspionieren. Die Kriminellen sammeln durch Spyware Daten und Informationen über Geräte oder Netzwerke, wie zum Beispiel Login- oder Standortdaten.

Adware: Hierbei handelt es sich um Programme, die dem Opfer ungewünschte Werbeanzeigen ausspielen.

Doch allein das Platzieren von Malware reicht den Kriminellen oft nicht. Sie möchten **Profit mit den gestohlenen Daten erwirtschaften**. Und da kommt der Begriff **Ransomware** ins Spiel.

Ransomware: Unter Ransomware versteht man eine bestimmte Form von Malware, die es zum Ziel hat, das Opfer durch Lösegeldforderungen unter Druck zu setzen und Geld zu erbeuten. Die Software verschlüsselt Daten des Opfers, sodass diese nicht mehr nutzbar sind. Die Kriminellen fordern im Anschluss ein Lösegeld, um die Daten freizugeben oder nicht im Darknet zu veröffentlichen. Ob diese nach Zahlung tatsächlich wie vereinbart behandelt werden, bleibt meist offen.

War auch Ihr Unternehmen schon einmal von einem Cyber-Angriff betroffen? Machen Sie jetzt einen mit CyberXperts. Vereinbaren Sie gerne ein persönliches Strategie-Beratungsgespräch – inklusive Live-Demo.

Die perfekte Tarnung: Über diese unscheinbaren Wege fangen wir uns Malware ein

Internet-Malware: Wie Downloads zum Verhängnis werden

Es vergeht kaum ein Tag ohne Meldungen über Angriffe mit Malware, die über gehackte Internetseiten oder über „Drive by Infektionen" ausgeführt werden. Häufig werden hierzu Internetseiten von bekannten Unternehmen gehackt und von dort wird die Malware zum Download angeboten.

Zwar muss der Nutzer noch aktiv einen Download ausführen, aber **er kann die Malware nicht erkennen, da der Download von einer vertrauenswürdigen Seite ausgeführt wird.**

Bei den „Drive by Infektionen“ werden den Unternehmen, die für die Einblendung der Werbebanner verantwortlich sind, Werbebanner untergeschoben, die mit der entsprechenden Malware infiziert wurden. So wird die Malware über Werbebanner auf „normalen“ Internetseiten im Hintergrund (Drive by) verteilt. **Eine „Drive by Infektion“ kann der Nutzer ebenfalls nicht erkennen.**

Der Trick mit den USB-Sticks: Dem Impuls, sie einzustecken und „mal schauen, was drauf ist“, kann keiner widerstehen

Nicht nur im Netz kann man sich Schadsoftware einfangen, sondern auch ganz analog. Angreifer nutzten diese Methode gezielt bei Unternehmen aus, um ahnungslose Mitarbeiter reinzulegen.

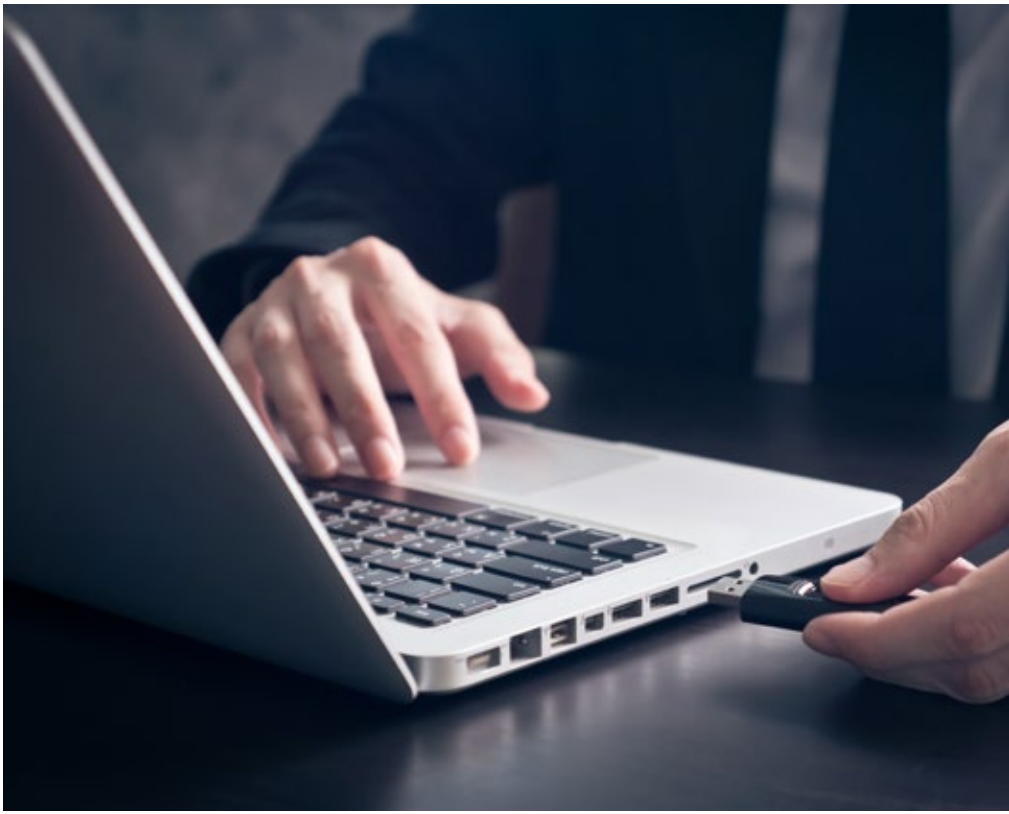
Dabei werden **präparierte USB-Sticks im Umkreis des Unternehmens ausgelegt**, meist mit dem eigenen Firmenlogo oder einem Namen eines Mitarbeiters (der ganz einfach über soziale Medien wie LinkedIn oder Xing auffindbar gemacht werden kann).

Mitarbeiter, die gerade auf dem Weg zur Arbeit sind, werden auf die USB-Sticks aufmerksam. Aus gutem Willen stecken sie den Stick ein, da sie denken, dass bestimmt ein Kollege den USB verloren habe.

Dabei greifen die Angreifer tief in die psychologische Trickkiste: Die natürliche Neugier des Menschen überwiegt hier und der Großteil der Opfer steckt die USB-Sticks in den eigenen PC, um zu sehen, was sich auf Ihnen befindet. Und dann ist es schon zu spät: Auf dem Stick befinden sich vorbereitete Dateien, die nur darauf warten, geöffnet zu werden und dadurch das Unternehmen zu infizieren.

Mein Tipp: Argumentieren Sie mit Schlagzeilen von „Conficker“, „Stuxnet“, „Wikileaks“, „Steuer-CDs“ und Datenschutzpannen mit verlorenen USB-Sticks. Prüfen Sie, ob zu jedem Zeitpunkt sichergestellt ist, dass auf jedem Rechner eine aktuelle Antivirensoftware und alle notwendigen Sicherheitspatches installiert sind. Auch wenn ein Rechner nach mehreren Wochen (Urlaub des Mitarbeiters) erstmals wieder angeschaltet und als Erstes ein USB-Stick eingesteckt wird: in den wenigsten Fällen wird man eine solche Zusicherung geben können.

Mein Tipp: Sie sollten primär prüfen, ob es offene Schnittstellen (USB-Ports, CD-Laufwerke) in Ihrem Unternehmen gibt und diese, wenn möglich, sperren lassen, damit Mitarbeiter sie gar nicht erst nutzen können



Vermeintliche Mitarbeiter: So einfach gelangen die Angreifer direkt ins Unternehmen

Und manchmal benötigt es gar keiner E-Mail oder keinen Datenspeicher, denn **die Angreifer kommen höchstpersönlich vorbei.** Diese geben sich dann als IT-Mitarbeiter oder Handwerker aus, kleiden sich passend und warten am Unternehmenseingang nur darauf, dass jemand die Tür nicht richtig schließt oder sie gar hereinbittet. Einmal im Unternehmen,

verschaffen sie sich einen Überblick und steuern dann direkt auf den Serverraum zu. Dort kann die Schadsoftware dann direkt im System platziert oder Unternehmensdaten abgezogen werden. Am Ende spazieren die vermeintlichen Mitarbeiter einfach wieder raus und der Schaden fällt oft viel später auf.

Tipp: Sensibilisieren Sie jetzt Ihre Mitarbeiter zu diesen Gefahren – mit den hoch-wirksamen E-Learnings von CyberXperts. Vereinbaren Sie gerne ein persönliches Strategie-Beratungsgespräch – inklusive Live-Demo.

Unser System verrät uns: Darum kennt Malware unsere Sicherheitslücken oft genau

Die Angreifer nutzen mit der Malware vorhandene Sicherheitslücken in den Betriebssystemen, Browsern, Java oder gängigen Softwareprodukten wie Acrobat Reader oder Office aus.

Wobei die Malware so hochentwickelt ist, dass sie **zunächst testet, welche Sicherheitslücke auf dem jeweiligen System vorhanden ist**, und erst dann die passende Malware installiert.

Antivirenprogramme sind gerade bei Malware, die vorhandene Sicherheitslücken ausnutzt, oftmals machtlos.

Die Malware führt in diesen Fällen in der Regel „erlaubte" Funktionen aus, die aber völlig andere Resultate liefern als erwartet. So kann der Angreifer nicht nur die Antivirensoftware überlisten, sondern mit den Rechten des angemeldeten Benutzers beliebige weitere Software aus dem Internet hochladen und installieren.

Mit dieser Methode kann der Angreifer das betroffenen IT-System komplett über- nehmen und fernsteuern.

Mein Tipp: Der sicherste Schutz für Ihr Unternehmen sind geschulte und sensibilisierte Mitarbeiter. Bauen Sie jetzt mit CyberXperts Ihre Human Firewall auf – hier Ihr unverbindliches Beratungsgespräch buchen!

Nur der richtige Antivirenschutz bringt wirklich etwas ... dieses eine (!) Kriterium muss er unbedingt erfüllen

Der Hauptanteil der Malware-Angriffe kommt noch immer über das Internet. Angesichts der Vielzahl von Malware ist ein funktionsfähiger Antivirenschutz unumgänglich.

Zur Erkennung von Cyberangriffen **ist neben dem klassischen Antivirenschutz auch eine sogenannte Malwareerkennung erforderlich**. Aktuelle Antivirensoftware haben solche Funktionen integriert.

Hier wird allzu oft **die Gefahr vernachlässigt, dass Angreifer die Malware über verschlüsselte Internetseiten (SSL, HTTPS) verteilen.**

Der Nutzer glaubt, damit ein hohes Maß an Sicherheit zu erhalten. In den wenigsten Unternehmen können diese verschlüsselten Downloads jedoch an zentraler Stelle nach Viren gescannt werden. Nur wenige Unternehmen sind bereit, die entsprechenden Investitionen zu tätigen, oder kennen überhaupt die Risiken.

Mein Tipp: Erarbeiten Sie mit der IT-Abteilung, dass in Ihrem Unternehmen der **Einsatz eines SSL-Proxys zum Scannen verschlüsselter Internetverbindungen nach Viren** geprüft wird.

Eine der wichtigsten Gegenmaßnahmen ist das regelmäßige „Patchen" von Sicherheitslücken.

Microsoft bietet für seine Produkte (Windows, Office usw.) automatische Updates an. Allerdings reicht es nicht nur, die Microsoft-Produkte auf dem neuesten Stand zu halten. Denn die Angreifer versuchen, Sicherheitslücken in allen Softwareprodukten auszunutzen.

Demnach müssen auch alle Softwareprodukte, die in Ihrem Unternehmen eingesetzt werden, regelmäßig mit Sicherheitsupdates versorgt werden. Dies ist allerdings in der Regel nur für aktuelle Betriebssystem- und Softwareversionen möglich.

Wichtig für die Geschäftsleitung: Setzen Sie in Ihrem Unternehmen ausschließlich aktuelle Betriebssystemversionen und aktuelle Softwareprodukte ein. Sie sparen ansonsten an der falschen Stelle. Das Risiko,

Opfer eines Angriffes durch ungepatchte Systeme zu werden, ist außerordentlich hoch.

Das wirtschaftliche Risiko eines Systemausfalls oder eines Spionageangriffs ist weitaus größer als die Investitionskosten für moderne Software.

Mein Tipp: Prüfen Sie, ob die automatische Aktualisierung auf allen Rechnern aktiviert ist bzw. ob alle Rechner von zentraler Stelle aus mit Sicherheitsupdates versorgt werden. Außerdem sollte die IT prüfen, ob wirklich alle Softwareprodukte mit Sicherheitsupdates versorgt werden.

9-teilige Checkliste: Haben Sie alle Maßnahmen zum Schutz vor Malware ergriffen?

Checkliste: Maßnahmen gegen Malware aus dem Internet	✔
Ist auf allen IT-Systemen (PC, Server, Mailserver usw.) eine Antivirensoftware installiert?	☐
Wird diese Antivirensoftware mindestens täglich automatisch aktualisiert?	☐
Werden alle IT-Systeme (Betriebssysteme) und alle Softwareprodukte regelmäßig und automatisiert mit Sicherheitsupdates versorgt?	☐
Wird das „Patchen“ der IT-Systeme und Softwareprodukte regelmäßig überwacht und dokumentiert?	☐
Wird der Internetzugang durch eine mehrstufige Firewall und einen zentralen Proxy-Server abgesichert?	☐
Werden alle Dateien vor dem Download an zentraler Stelle nach Viren gescannt?	☐
Werden auch Downloads über verschlüsselte Verbindungen (SSL, TLS) an zentraler Stelle nach Viren gescannt?	☐
Werden ausschließlich Betriebssysteme und Softwareprodukte eingesetzt, für die es noch Sicherheitsupdates seitens des Herstellers gibt?	☐
Ist die Geschäftsführung über die Risiken durch Malware informiert?	☐

Alle 22 Sekunden wird eine neue Malware in Umlauf gebracht, die auf Android-Geräte zielt. Bei der Gefahrenabwehr kommt es zu fast 100 % auf das Verhalten der Mitarbeiter an. Schützen Sie Ihre Systeme jetzt mit einer Sensibilisierungs-Kampagne von CyberXperts.

Sperrangelweit offen: So einfach macht die Nutzung von Smartphones es den Cyber-Angreifern

Smartphones sind heutzutage hinsichtlich ihres Funktionsumfangs **mit Notebooks zu vergleichen**:

- Sie verfügen standardmäßig neben der Telefonfunktion über einen Internetbrowser, E-Mail-Kommunikation, Textverarbeitung, Spracheingabe, Dateiverwaltung
- und können durch eine Unzahl weiterer Apps nahezu beliebig erweitert werden.

- Im Gegensatz zu einem Notebook sind Smartphones ständig mit dem Internet verbunden.

Im privaten Umfeld werden über das Smartphone auch **Bankgeschäfte abgewickelt**, was diese Geräte insbesondere für Angriffe auf das Onlinebanking interessant macht.

Malware versendet auch kostenpflichtige SMS, stiehlt personenbezogene Daten und ruft kostenpflichtige Rufnummern an.

Da die meisten Nutzer mit dem Smartphone aber auch **auf ihre geschäftlichen E-Mails und Unternehmensdaten zugreifen**, sind sie auch Ziel von Spionageangriffen.

Mein Tipp: Sie müssen besonderes Augenmerk auf Sensibilisierungsmaßnahmen legen, da es kaum technische Möglichkeiten gibt, die Nutzer vor ihrer eigenen Leichtfertigkeit zu schützen. Schulen Sie Ihre Mitarbeiter jetzt umfassend zum Umgang mit mobilen Endgeräten und vermeiden Sie Angriffe auf Ihr Unternehmen!

Warum selbst zertifizierte Software aus App-Stores keinen 100-%-Schutz bietet

Die Angriffsmethoden auf Smartphones folgen denen auf PCs oder Notebooks. Allerdings gibt es auf den Smartphones seitens der Hersteller bereits Sicherheitsmechanismen, die Angriffe mit Malware verhindern können.

Das wesentlichste Sicherheitskonzept ist in diesem Zusammenhang, dass nur zertifizierte Software auf den Geräten installiert werden kann. Die Hersteller bieten in ihren App-Stores ausschließlich geprüfte Software bereit. Im Vordergrund steht nicht die Einhaltung datenschutzrechtlicher Anforderungen, sondern ausschließlich die Datensicherheit. Zudem werden immer wieder Apps in die Stores der Hersteller eingeschleust, die mit Malware infiziert wurden.

Darum gibt es immer mehr Malware für Android-Geräte

Das Sicherheitsunternehmen Kaspersky Lab schreibt in seinem Bericht zur Bedrohungslage von Smartphones, dass *„Die Entwicklung mobiler Malware – vor allem für Android – rasant voranschreitet“*.

Denn Android bietet Cyberkriminellen zahlreiche Möglichkeiten – das Betriebssystem ist weit verbreitet und sowohl für App-Entwickler als auch **für Virenschreiber leicht zu nutzen**.

Zudem werden in der Regel Android-Geräte von den Herstellern nur zwei Jahre mit Sicherheitsupdates versorgt. Das führt dazu, dass **eine Vielzahl älterer Geräte genutzt wird**, die über **massive Sicherheitslücken** verfügen. Solche Geräte können von Cyberkriminellen leicht übernommen werden und sollten **im Unternehmensumfeld in keinem Fall genutzt werden**.

Wichtig für den IT-Sicherheitsbeauftragten: Angesichts dieser Bedrohungslage ist der Einsatz von Android-Geräten im Unternehmensumfeld als kritisch zu betrachten. Ohne zusätzliche Sicherheitsmaßnahmen können Sie dem Einsatz solcher Geräte nicht zustimmen

Ist einmal Malware auf dem Gerät installiert, können die Angreifer **beliebige weitere Malware nachinstallieren**, sodass die Risiken nicht mehr einzugrenzen sind.

Da Android ein offenes System ist, **kann jede Malware** – gerade bei einem gerooteten System – auch **ungehindert auf alle Daten zugreifen**.

Rooten: Beim „Rooten“ oder „Jailbreak“ (iOS) werden die Sicherheitsmechanismen des Betriebssystems durch den Einsatz spezieller Tools ausgehebelt. Der Nutzer installiert diese meist ohne Wissen durch nur einen Klick. Der Angreifer kann dann auch wesentliche Sicherheitseinstellungen des Betriebssystems ausschalten.

Das große Hersteller-Versagen: Warum Android-Handys bei der Sicherheit oft Lücken haben

Auch Smartphones haben Betriebssysteme und Softwareprodukte, die Sicherheitslücken enthalten können. Deshalb ist es für die Abwehr von Malwareangriffen von entscheidender Bedeutung, dass diese Geräte regelmäßig mit Sicherheitsupdates versorgt werden.

Bei iOS-Geräten wird dies – ähnlich wie bei Microsoft-Systemen – zentral von Apple über automatische Updates gesteuert.

Bei Android-Geräten ist dies leider noch immer nicht der Fall. Android wird von unterschiedlichsten Geräteherstellern auf verschiedene Geräte angepasst und kann daher nicht mehr zentral mit Sicherheitsupdates

versorgt werden. Eine aktuelle Android-Version kann demnach nur der Kunde erhalten, der ein neues Gerät kauft. Aber selbst dann kann dieses Gerät im nächsten Monat schon eine gravierende Sicherheitslücke haben, die vom Gerätehersteller nicht gepatcht wird.

Im betrieblichen Umfeld können ein solches Verfahren und die daraus resultierenden Risiken nicht toleriert werden.

Mein Tipp: Wirken Sie darauf hin, dass auf betrieblichen Smartphones ausschließlich Apps installiert werden, die für die betriebliche Nutzung erforderlich sind. Das reduziert das Risiko, Opfer von Datendiebstahl zu werden, erheblich. Wichtig ist es hierbei, auch den Mitarbeitern den Ernst der Lage zu verdeutlichen. Mit interaktiven E-Learnings schulen Sie Ihre Mitarbeiter wirksam für die Verwendung von Smartphones im betrieblichen Umfeld.

Wichtiger Baustein Ihrer Gefahrenabwehr: Mit ein paar einfachen technischen Maßnahmen schützen Sie Notebooks & Tablets

Notebooks, PCs und Tablets sind Malwareangriffen ausgesetzt. Typische Angriffe laufen über das Internet, E-Mail und USB-Datenträger. Allerdings können Angreifer mobile Geräte sehr viel leichter in die Hände bekommen als PCs in Ihrem Unternehmen.

Ein erhebliches Risiko stellt also der Verlust oder der temporäre Zugriff eines Angreifers auf ein mobiles Gerät dar.

Hat der Angreifer Zugriff auf das Gerät, kann er nicht nur Informationen stehlen, sondern das Gerät auch mit Malware infizieren, die es ihm er-

möglicht, zu einem späteren Zeitpunkt in Ruhe weitere Angriffe über das Internet durchzuführen und sogar in Ihr Firmennetzwerk einzudringen.

Ein Angreifer benötigt zum Kapern eines Notebooks ohne Passwort mit einem CD-Laufwerk ungefähr 5 Minuten! Hierzu sind noch nicht einmal besondere IT-Kenntnisse erforderlich. Es reicht eine Linux-CD.

Mein Tipp: Schützen Sie mobile Geräte vor solchen Angriffen. Das können Sie durch eine Festplattenverschlüsselung, sichere Zugangskennwörter für den Systemstart und andere einfache technische Maßnahmen erreichen.

Moderne Geräte haben solche Sicherheitsmaßnahmen oftmals bereits in die Hardware (BIOS, Festplatten) oder Betriebssysteme (Systemverschlüsselung bei iOS-Geräten) integriert.

So bieten die meisten Hersteller Notebooks mit Festplatten an, die über eine **interne Verschlüsselung** verfügen oder **Gerätesperren, die bereits vor dem Systemstart greifen**. Solche Systeme kosten unwesentlich mehr, schützen aber sehr wirksam vor Datenverlust.

Wichtig für die Geschäftsleitung: Sicherheit gibt es nicht zum Nulltarif. Aber die Investitionskosten für sichere Geräte sind bei Weitem geringer als ein erfolgreicher Angriff über ein infiziertes Notebook auf Ihr Unternehmensnetzwerk. Allein der Schaden bei dem Verlust eines Notebooks mit vertraulichen Daten aus der Entwicklungsabteilung kann Sie sehr viel Geld kosten.

Checkliste sicheres Passwort	✔
Mindestens 8 Zeichen lang	☐
Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen	☐
Keine Namen von Familienmitgliedern, Geburtsdaten oder andere leicht zu erratende Begriffe	☐
Unterschiedliche Passwörter für unterschiedliche Accounts	☐

Nutzen Sie zur Erstellung und zum sicheren Versenden von Zugangsdaten auch unseren kostenfreien Passwort-Generator: PrivacyXperts – Passwörter erstellen & senden.

Fiese Fallen: Wenn die Teams-Mitteilung voller Malware steckt

Neben dem Internet ist die E-Mail einer der Hauptangriffswege für die Verteilung von Malware. Jedes Unternehmen wird von E-Mails überflutet und die Mitarbeiter sind angesichts der E-Mail-Massen oftmals überfordert und unaufmerksam.

Angreifer haben daher leichtes Spiel, da die Opfer zudem i.d.R. neugierig und allzu leichtgläubig sind.

Es genügt ein Klick auf einen infizierten Anhang oder einen Link auf eine gehackte Seite und der PC ist infiziert.

Der Anwender hat in der Regel keine Chance, einen solchen Angriff im Vorhinein zu erkennen.

Wird ein Angriff über E-Mail noch mit den Mitteln des Social Engineerings verknüpft, sind die Erfolgsaussichten sehr hoch. Denn das Opfer glaubt sich in der Regel bei solchen Angriffen in vermeintlicher Sicherheit, weil es den Absender der E-Mail kennt und als vertrauenswürdig einstuft.

Mein Tipp: Der beste Schutz vor betrügerischen E-Mails ist die Mitarbeitersensibilisierung. Mit CyberXperts simulieren Sie Phishing-Kampagnen, klären auf und sorgen für eine langanhaltende Awareness bei den Beschäftigten. Vereinbaren Sie jetzt einen unverbindlichen Beratungstermin für Ihre Phishing-Simulation!

Sie können E-Mails durch einfache, klare Regeln sicherer machen. Veröffentlichen Sie z. B. die nachfolgenden E-Mail-Tipps in Ihrem Intranet.

Muster Mitarbeiterinformation: E-Mails, aber sicher!

E-Mails können Schadprogramme enthalten und deshalb Risiken und Gefahren für unser Unternehmen, Ihre Arbeitsstation oder Ihre Daten darstellen. Beachten Sie deshalb Folgendes:

- Vertrauen Sie grundsätzlich nur solchen E-Mails, deren Absender Sie zweifelsfrei kennen.
- E-Mails von zweifelhafter Herkunft sind ungeöffnet zu löschen.

- Öffnen Sie keine Anhänge von E-Mails, deren Absender Sie nicht kennen.
- Klicken Sie nicht auf Links in E-Mails, deren Absender Sie nicht kennen. Überlegen Sie immer, ob der Link oder der Dateianhang in den Kontext der E-Mail und den Geschäftsvorgang passt.
- Ungeöffnet zu löschen sind immer Anhänge wie Bildschirmschoner (Dateien mit der Endung «.scr»), ausführbare Dateien («.exe», «.bat», «.vbs» etc.) und Bilder (jpg, tif, gif, bmp) von zweifelhafter Herkunft.
- Bei Anfragen per E-Mail hat man grundsätzlich keinerlei Gewissheit über die Identität des Absenders, da der Sender die Informationen über seine Identität problemlos beliebig selbst definieren kann. Im Zweifelsfall müssen Sie beim angegebenen Absender telefonisch nachfragen.
- Schränken Sie automatische Antworten auf nur Interne oder Ihre Kontaktpersonen ein. Niemand sonst muss wissen, wenn Sie länger weg sind.

Eine weitere Gefahr: Botnets!

Angriffe mit Schadsoftware, beispielsweise über E-Mails, sind schon übel genug. Botnet-Angriffe sind aber mindestens genauso ärgerlich.

Botnet ist ein Koffer- oder Schachtelwort und setzt sich aus Roboter und Network zusammen. Computer werden dabei zu Verteilernetzwerken zusammengefasst und agieren wie ein Roboter.

Verteilernetzwerke sind per se nichts Schlimmes. Sie dienen dazu, eine Reihe von Computern zu einem Netzwerk zusammenzufassen. Diese Verteilernetzwerke werden auch Peer-to-Peer-Netzwerke genannt und dienen dazu, Daten im Internet bereitzustellen. Die infizierten Computer agieren in einem Botnet ferngesteuert und verteilen dann Spam oder Schadsoftware.

Für Ihr Unternehmen kann das äußerst unangenehm sein. Die folgende Checkliste hilft Ihnen, infizierte Computer zu erkennen und im Vorfeld dafür zu sorgen, dass sich Schadsoftware nicht verbreiten kann:

Checkliste: Infizierte Computer erkennen

Maßnahmen	Bedeutung
Setzen Sie einen Sicherheitsscanner ein.	Die bekanntesten Hersteller von Antiviren-Software stellen kostenlose Viren-Scanner zur Verfügung, mit denen Sie Ihr System über das Internet gratis prüfen können. Einige dieser Hersteller stellen darüber hinaus Sicherheitsinformationen auf eigenen Cloud-Servern zur Verfügung. Die wichtigsten Scanner in alphabetischer Reihenfolge sind: ■ Bitdefender Quick Scan ■ ESET Online Virenscanner ■ F-Secure Online-Scanner ■ Kaspersky Online-Scanner ■ McAfee Security Scan Plus ■ Trend Micro HouseCal
Prüfen Sie Ihre Computer mit einem speziellen Scanner	In Zusammenarbeit mit dem Verband der deutschen Internetwirtschaft e.V., dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesministerium des Innern wurde das Programm DE-Cleaner entwickelt, mit dem Sie Botnetze aufspüren und eliminieren können. Der Nachfolger heißt HitmanPro. EU-Cleaner und wird als 30 Tage-Testversion bereitgestellt. Das Programm gibt es jeweils in einer Variante der Firmen Avira, von Kaspersky und von Symantec. Bevor Sie das Programm starten, sollten Sie die wichtigsten Daten Ihres PCs sichern, indem Sie sie auf einem USB-Stick speichern oder auf einem zentralen Server ablegen. Nach der Installation werden Sie aufgefordert, die Bereiche auszuwählen, die gescannt werden sollen. Sie sollten hier auf jeden Fall Autostart-Objekte, den Systemspeicher und die Bootsektoren untersuchen lassen. Nach dem Scanvorgang zeigt das Programm an, ob irgendwelche Malware – also Schadsoftware – gefunden wurde. Sie sollten diese Programme auf jeden Fall löschen, so wie es empfohlen wird.

Maßnahmen	Bedeutung
Installieren und konfigurieren Sie ein zentrales Gateway.	Ein zentrales Gateway ist dazu in der Lage, ein- und ausgehenden Datenverkehr zu filtern und Angriffe zu lokalisieren. Ein solches Gateway ist darüber hinaus auch in der Lage, den Datentransfer zu filtern, der von Botnetzen ausgeht. 2 empfehlenswerte Gateways sind die auf Linux basierenden IPCop und Endian. Beide Systeme sind kostenlos und bringen ein eigenes Linux Betriebssystem mit. Ein zusätzlicher Vorteil ist, dass Sie einen Computer verwenden können, den Ihr Unternehmen längst ausmustern wollte. Für diese Gateways benötigen Sie keine Highend-Hardware.
Filtern Sie Ihre E-Mails zentral nach Spam und Schadsoftware.	Die meisten Firmen rufen Ihre E-Mails von einem zentralen Server eines Webproviders ab. Sprechen Sie mit Ihrem Provider und fragen Sie dort nach, ob er E-Mails nach von Ihnen vorgegebenen Kriterien filtern kann. Wenn Sie einen Microsoft Exchange Server im Einsatz haben, sollten Sie den Forefront Security für Exchange Server (FSE) installieren. Das Programm unterstützt die Server-Versionen ab 2003 und schützt Ihr Unternehmen vor Viren, Spam und anderer Malware, die mit E-Mails verschickt und empfangen werden.
Installieren Sie regelmäßig die neusten Sicherheitspatches und die neusten Updates.	Da in Betriebssystemen und in Standardsoftware ständig Sicherheitslücken aufgespürt werden, müssen permanent Sicherheitspatches installiert werden, die diese Lücken schließen. Prüfen Sie, ob in Ihrem Unternehmen das Betriebssystem und die Standardsoftware auf dem neuesten Stand sind. Sicherheitspatches und Updates können in kleineren und größeren Unternehmen zentral über einen Server installiert werden. So muss der Administrator nicht jeden Computer einzeln überprüfen. Seitdem Windows 10 halbjährlich komplett aktualisiert wird, ist es empfehlenswert die halbjährlichen Updates regelmäßig durchzuführen. Microsoft stellt nämlich den Support für ältere Updates nach einer gewissen Zeit ein.

Mit dieser Checkliste spüren Sie Sicherheitslücken in Ihrem Unternehmen auf

Trotz Virenscanner und eingerichteter Firewall erleben wir es immer wieder, dass in Unternehmen die simpelsten Schutzmaßnahmen nicht getroffen werden. Zu diesen gehören unter anderem eine regelmäßige Datensicherung und eine unterbrechungsfreie Stromversorgung.

Checkliste: Sind alle Sicherheitsmaßnahmen getroffen?	
Netzsicherheit erledigt?	✔
Sicherheitsmaßnahmen gegen Malware (Virenschutz, Trojaner-Detektion, Spam-Schutz etc.)	☐
Sicherheitsmaßnahmen gegen netzbasierte Angriffe (IPS/IDS-Systeme, Firewall, Application Layer Gateway etc.)	☐
Geeignete Netzsegmentierung (Isolierung des Management-Netzes vom Datennetz)	☐
Sichere Konfiguration aller Komponenten (unnötige Ports und Dienste deaktivieren, Einrichten eines VLAN)	☐
Fernadministration durch einen sicheren Kommunikationskanal (z. B. SSH, IPSec, TLS/SSL, VPN)	☐
Verschlüsselte Kommunikation aller Komponenten, die mit dem Internet kommunizieren (z. B. TLS/SSL)	☐
Verschlüsselte Kommunikation mit Drittdienstleistern, falls diese für das eigene Angebot notwendig sind	☐
Redundante Vernetzung der Switches	☐
Serversicherheit erledigt?	✔
Technische Maßnahmen zum Schutz der Server (Host Firewalls, regelmäßige Integritätsüberprüfungen, Hostbased Intrusion Detection Systems)	☐
Sichere Grund-Konfiguration der Server (z. B. Einsatz gehärteter Betriebssysteme, Deaktivierung unnötiger Dienste etc.)	☐
Regelmäßige Datensicherung aller Daten, Programme, Datenbanken und Dienste. Einübung der Wiederherstellung	☐

Remoteadministration der Server über sichere Kommunikationskanäle (RDP, VPN)	☐
Segmentierung der Servernetzwerke über DMZ	☐
Datensicherheit erledigt?	✔
Datensicherheit im Lebenszyklus der Unternehmensdaten definieren und umsetzen	☐
Sichere Isolierung der sicherheitsrelevanten Daten (z. B. virtuelle Speicherbereiche, Tagging etc.)	☐
Regelmäßige Datensicherungen, deren Rahmenbedingungen (Umfang, Speicherintervalle, Speicherzeitpunkte und Speicherdauer) nachvollziehbar sind	☐
Personenbezogene Daten müssen auf Wunsch der Mitarbeiter vollständig und zuverlässig gelöscht werden	☐
Rechenzentrumssicherheit erledigt?	✔
Redundante Auslegung aller wichtigen Versorgungskomponenten (Strom, Klimatisierung der RZ, Internetanbindung, Verkabelung etc.)	☐
Überwachung des Zutritts: Zutrittskontrollsystem, Videoüberwachungssysteme, Bewegungssensoren, Sicherheitspersonal, Alarmsysteme etc.	☐
Zwei-Faktor-Authentisierung für den Zugang zu Servern und den Zutritt ins Rechenzentrum	☐
Brandschutz: Brandmeldeanlage, Brandfrüherkennung, geeignete Löschtechnik, regelmäßige Brandschutzübungen	☐
Robuste Infrastruktur, die ausreichenden Widerstand gegen Elementarschäden und unbefugtes Eindringen bietet (Stahltüren, vergitterte Fenster etc.)	☐
Redundante Rechenzentren durch den Einsatz von virtuellen Servern in der Cloud	☐

Wollen auch Sie wissen, wie gut Ihre Datensicherheit aufgestellt ist? Machen Sie jetzt einen 360°-Check Ihrer Sicherheitslage mit CyberXperts. Vereinbaren Sie gerne ein persönliches Strategie-Beratungsgespräch – inklusive Live-Demo.

Ernstfall Angriff: Setzen Sie 5 Schritte direkt um

Da es keine absolute Sicherheit gibt, müssen Sie sich auf den Ernstfall vorbereiten. Sie brauchen in Ihrem Unternehmen **klare Handlungsanweisungen** und **definierte Prozesse**, um im Schadenfall tatsächlich Erste Hilfe leisten zu können.

Vorbereitung ist alles: Bereiten Sie Ihr Unternehmen auf den Ernstfall vor

Tritt ein Sicherheitsvorfall auf, müssen Sie mit dem Ausfall wesentlicher IT-Systeme und einem vollständigen Ausfall zentraler Geschäftsprozesse und Fertigungsketten rechnen. Das kann schnell zu einem kompletten **Betriebsausfall über mehrere Wochen** führen:

- Bei einem Ransomware-Angriff müssen z. B. regelmäßig sämtliche IT-Systeme komplett ausgetauscht werden. Das betrifft auch vermeintlich „saubere“ IT-Systeme.
- Zudem müssen bei einem Betriebsausfall regelmäßig die **Kunden**, die **Presse** sowie Ihre **Kolleginnen und Kollegen** informiert werden.
- Sind personenbezogene Daten betroffen, müssen Sie auch die **Aufsichtsbehörde** innerhalb von 72 Stunden informieren. Hier sind Datenschutzbeauftragte ganz konkret involviert.
- Bei einem Sicherheitsvorfall müssen meistens **externe Spezialisten hinzugezogen** werden. All diese Maßnahmen müssen koordiniert und sachgerecht umgesetzt werden. Weisen Sie deshalb Ihre Geschäftsführung und Ihre IT-Abteilung auf die Risiken hin.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht regelmäßig einen umfassenden Leitfaden, der die zentralen Maßnahmen bei einem Sicherheitsvorfall beschreibt. Hier sind die wichtigsten Schritte:

Handlungsleitfaden im Notfall – mit diesen 5 Schritten handeln Sie richtig

Schritt 1: Sachlage beurteilen

Die Entscheidung, ob es sich bei dem jeweiligem Ereignis um einen IT-Sicherheitsvorfall oder um eine IT-Störung handelt, ist nicht immer eindeutig zu treffen.

Viele Angriffe werden erst nach einigen Tagen oder gar Wochen erkannt.

Umso wichtiger ist es, Auffälligkeiten zu erkennen und sie zu melden. Die Beurteilung der Sachlage obliegt nach der Meldung den Sicherheitsexperten.

Schritt 2: Melden

- Ruhe bewahren und nicht übereilt handeln
- Netzwerkkabel des IT-Systems ziehen
- keinesfalls das IT-System ausschalten
- sicherheitsrelevantes Ereignis melden

Schritt 3: Prüfung der Sicherheitsmeldung

- Das IT-Notfallteam prüft die Meldung und schätzt die Sachlage ab. Werden zur Beurteilung weitere Spezialisten aus den jeweils betroffenen Fachabteilungen benötigt, werden diese unverzüglich zusammengerufen.
- Wird ein IT-Sicherheitsvorfall festgestellt, ist der ISB unverzüglich zu informieren.
- Die IT-Abteilung oder der **Informationssicherheitsbeauftragte (ISB)** , wenn vorhanden, prüft die Meldung und schätzt die Sachlage ab.
- Wurde bei der Prüfung kein IT-Sicherheitsvorfall festgestellt, gibt der ISB die Bearbeitung des Vorfalls in den zuständigen Fachbereich zur weiteren Bearbeitung ab.

Schritt 4: Technische Sofortmaßnahmen

- **Oberste Regel:** Keinesfalls darf eine Anmeldung mit privilegierten Nutzerkonten (Administratorkonten) auf einem potenziell infizierten System erfolgen, während das System sich noch im internen produktiven Netzwerk befindet oder mit dem Internet verbunden ist!
- Potenziell infizierte Systeme müssen umgehend vom Netzwerk isoliert werden, um eine weitere Ausbreitung der Schadsoftware im Netz durch Seitwärtsbewegungen (Lateral Movement) zu verhindern.
  - Dazu das Netzwerkkabel ziehen.
  - Gerät nicht herunterfahren oder ausschalten.

- Ggf. forensische Sicherung inkl. Speicherabbild für spätere Analysen (eigene, durch Dienstleister oder Strafverfolgungsbehörden) erstellen.

- **Das/die Schadprogramm/e müssen identifiziert werden.** Für Ransomware können etwa die Seiten „No More Ransom“ und „ID Ransomware“ genutzt werden. Sollte es für die Ransomware bereits Entschlüsselungstools geben, wird dies dort angezeigt – die Wahrscheinlichkeit hierfür ist jedoch gering. Ebenso sollte beim S-CERT eine Meldung über die Schadsoftware erfolgen (siehe auch „Externe Unterstützung“).

- In einigen Fällen steht der Name der Ransomware auch in dem üblicherweise angezeigten Erpresserschreiben oder er wird den verschlüsselten Dateien als Dateinamenserweiterung hinzugefügt.

- Zu einer bekannten Ransomware können dann mithilfe gängiger Suchmaschinen Informationen gefunden werden.

- Die Schadprogramme nehmen teilweise tiefgreifende (sicherheitsrelevante) Änderungen am infizierten lokalen System vor, die nicht einfach rückgängig gemacht werden können. **Das BSI empfiehlt daher grundsätzlich, infizierte lokale Systeme als vollständig kompromittiert zu betrachten und neu aufzusetzen.**

- Fortschrittliche Schadsoftware-Varianten wie Trickbot können sich mit ausgespähten Zugangsdaten für Benutzerkonten (ggf. mit administrativen Rechten) lateral im Netzwerk ausbreiten. Zu beachten ist die Problematik eines „Golden Tickets“ und Kompromittierungen von Domaincontrollern und Serversystemen (Active Directory und alle Domain-joined-Systeme neu aufsetzen).

- Sollte das nicht schnell möglich sein, muss das Passwort des eingebauten Key Distribution Service Accounts (KRBTGT) zweimal zurückgesetzt werden. Dies invalidiert alle Golden Tickets, die mit dem zuvor gestohlenen KRBTGT-Hash und allen anderen Kerberos Tickets erzeugt wurden.

- Alle auf betroffenen Systemen gespeicherten bzw. nach der Infektion eingegebenen Zugangsdaten müssen als kompromittiert betrachtet und die Passwörter geändert werden. Dies umfasst u. a. Webbrowser, E-Mail-Clients, RDP/VNC-Verbindungen sowie andere Anwendungen wie PuTTY, FileZilla, WinSCP etc.

- Jede nicht unbedingt benötigte Remote-Verbindung ist zu blockieren, der Netzwerkverkehr ist zu beobachten und Antiviren-Scans sind durchzuführen, um weitere Infektionen und Täterzugriffe auszuschließen.
- Es muss unverzüglich geprüft werden, ob saubere, integre Backups vorhanden sind.
- Im Fall einer bereits erfolgten Verschlüsselung sollte grundsätzlich nicht auf die Erpressung eingegangen werden und **es sollte kein Lösegeld bezahlt werden**. Stattdessen sollten die Daten in ein sauberes Netzwerk aus Backups zurückgespielt werden.
- Eine Persistenz von Schadsoftware im BIOS oder gar der Hardware ist sehr selten und wird bislang nicht von breit verteilter Schadsoftware angewandt.
- Um einen zukünftigen weiteren Zugriff der Täter auf das interne Netzwerk und eine erneute Ausbreitung von Schadsoftware auszuschließen, muss im Fall einer Kompromittierung des AD das Netz unbedingt komplett neu aufgebaut werden. Dies kann nach einer schnellen Bereinigung unter Umständen auch langfristig nach Sicherstellung der Betriebsfähigkeit erfolgen.

Schritt 5: Einberufung von „Projektteam IT-Sicherheitsvorfall“

Wurde bei der Prüfung ein IT-Sicherheitsvorfall festgestellt, beruft der ISB das Projektteam ein. Der ISB informiert unverzüglich die Unternehmensleitung.

Der ISB organisiert unverzüglich das erste Treffen des Projektteams. Hierbei sind folgende Themen zu klären:

- Wer macht was bis wann?
- Welche Tagesaufgaben können für die Bewältigung des Vorfalls liegen gelassen werden?
- Wer trifft die relevanten Entscheidungen?
- Sollen Systeme schnell wieder aufgesetzt oder Spuren gesichert werden?
- Wer kommuniziert was wann an wen?

- Soll Anzeige erstattet werden?
- Sind externe Dienstleister zu benachrichtigen?
- Sind Meldepflichten zu beachten?
- Ist externe Unterstützung erforderlich?

Kurzfristig für den Notbetrieb erforderliche Daten können sich auch an gegebenenfalls abgesetzten Außenstellen oder auf Systemen von Mitarbeitern im Urlaub befinden, welche (noch) nicht betroffen sind. Diese sind unverzüglich zu benachrichtigen.

Sollten sich Anzeichen ergeben, die darauf schließen lassen, dass zeitkritische Prozesse über den im Notfallmanagement definierten Zeitraum hinweg ausfallen, ist der BCM-Koordinator zu informieren.

Dieser aktiviert in Abstimmung mit dem BCM-Beauftragten gegebenenfalls den Notfallplan gemäß dem Notfallhandbuch. Der ISB informiert die Geschäftsleitung fortlaufend über den aktuellen Stand der Maßnahmen.

Mein Tipp: Eine Cyber-Versicherung ist sinnvoll. Cyber-Versicherungen bieten in der Regel bei einem Sicherheitsvorfall auch Unterstützung durch Spezialistenteams an. Für den Abschluss solcher Versicherungen wird häufig eine Phishing-Simulation gefordert. Lassen Sie sich jetzt kostenfrei beraten, wie Sie mit wenig Aufwand und trotzdem großer Wirksamkeit Phishing-Simulationen in Ihrem Unternehmen durchführen!

Fazit: Sie müssen vorbereitet sein

Wirken Sie darauf hin, dass sich Ihr Unternehmen auf einen Sicherheitsvorfall vorbereitet. **Das BSI bietet mit dem Standard 100-4 (BCM) und dem Leitfaden „Erste Hilfe bei einem Sicherheitsvorfall“ sehr gute Unterstützung.**

Weisen Sie auf die Risiken hin und machen Sie Ihren Stakeholdern verständlich, dass die Risiken nur mit sachgerechten Standardprozessen und Maßnahmen minimiert werden können. Das bedeutet aber einen erheblichen Arbeitsaufwand von mehreren Monaten für die Einführung und viel Aufwand für den nachfolgenden Linienbetrieb. Auch darauf müssen Sie hinweisen.

Awareness ist Trumpf: So sensibilisieren Sie Ihre Mitarbeiter für die Malware-Bedrohung

Mitarbeiter sind noch immer das größte Einfallstor für Angreifer auf Ihr Unternehmen. Wirksam geschulte Mitarbeiter sind daher Ihre Human Firewall vor Angriffen! Wichtig ist dabei, dass Sensibilisierung zur Routine wird, denn im Arbeitsalltag gehen komplizierte Regelungen schnell unter.

CyberXperts ist die Lösung für Ihre IT-Sicherheit. Wir vereinen die 3 wichtigsten Säulen des IT-Schutzes für Sie: eine starke Mitarbeitersensibilisierung, ein sicheres System und ein dauerhafter Check Ihrer Unternehmenssicherheit vor neuen Bedrohungen. Schützen Sie Ihr Unternehmen mit CyberXperts messbar!

Modul 1: Mit diesen stets aktuellen Schulungsvorlagen sensibilisieren Sie Ihre Mitarbeiter wirksam für Cyber-Fallen!

Ihre Mitarbeiter sind Ihre Human Firewall und schützen Ihr Unternehmen. Schulungslücken und fehlende Awareness sind das größte Risiko für Sie. Zeitdruck und Unvorsichtigkeit im Berufsalltag sind das Einfallstor für Angreifer.

Sicher ist Ihr Unternehmen nur, wenn Awareness zur Routine wird.

Mit dem starkem Bild- und Videomaterial von CyberXperts sensibilisieren Sie Ihre Mitarbeiter wirksam und langanhaltend.

Stets aktuelle Schulungen sorgen dafür, dass Ihre Mitarbeiter bei den ständig neuen Bedrohungen immer auf dem neuesten Stand sind.

Dabei gehen wir bei CyberXperts nach diesen Prinzipien vor:

- **Positives Reinforcement:** Kontinuierliche Schulungs-Einheiten sorgen für einen nachhaltigen Lern-Effekt
- **Kein trockenes E-Learning, kein Frust:** Gamifizierung und Interaktion bringen Interesse und Motivation.

- **Echte Beispiele aus der Realität:** Reale Situationen unterstreichen die Relevanz des Themas und zeigen, wie raffiniert Cyberkriminelle vorgehen!
- **Maßgeschneidert für Ihr Unternehmen** Unser E-Learning können Sie mit Ihrem Unternehmenslogo individualisieren und an Ihre Corporate Identity anpassen.

Modul 2: Die perfekte Phishing-Simulation: So identifizieren Sie Schulungs-Potenzial und erhalten einen Nachweis für die ISO 27001

Mit simulierten Phishing-E-Mails lernen Ihre Mitarbeiter effektiv Angriffe zu erkennen und im Ernstfall richtig zu reagieren. Die automatisierten Phishing-Kampagnen von CyberXperts können Sie individuell an Ihr Unternehmen anpassen und aussteuern.

Ihre Auswertung zeigt Ihnen das Schulungspotential und kann als **Nachweis für Cyber-Versicherungen und die ISO 27001** genutzt werden.

So geht's:

Wir besprechen in einem persönlichen Gespräch mit Ihnen wie Ihre persönliche Kampagne aufgesetzt werden soll: Sie wählen, ob alle oder nur einzelne Abteilungen E-Mails erhalten und in welchem Abstand. Für eine möglichst realistische Simulation berücksichtigen wir, welche Tools und Software in Ihrem Unternehmen standardmäßig verwendet werden.

1. **Let's phish! Die Test-E-Mails gehen raus.** Nachdem Ihre Kampagne eingerichtet wurde, versenden Sie eine unangekündigte Test-Phishing-E-Mail, die Sie zum Startschuss Ihrer Kampagne machen. Danach werden in regelmäßigen Abständen simulierte Phishing-E-Mails automatisiert an Ihre Mitarbeiter versendet. Sie brauchen sich um nichts mehr zu kümmern. Falls ein Mitarbeiter klickt, erhält er einen Hinweis und kann direkt lernen, wie er eine solche Panne beim nächsten Mal vermeiden kann.
2. **Eine automatische Auswertung Ihrer Phishing-Kampagne wird für Sie generiert.** Hier erfahren Sie, wie viel Prozent Ihrer Mitarbeiter geklickt haben und in welchen Abteilungen Schulungsbedarf besteht.

Jetzt gratis Phishing-Simulation für Ihr Unternehmen durchführen: Reservieren Sie einfach hier Ihr persönliches Strategie-Gespräch!

Mit einer Phishing-Simulation sorgen Sie für einen starken Aha-Effekt bei Ihren Mitarbeitern … und einer hohen Bereitschaft dafür, sich mit dem Thema CyberSecurity auseinanderzusetzen.

Modul 3: Mit einem intuitivem 360°-Check zur Einschätzung Ihres Risikoprofils kennen Sie die Sicherheitslage Ihres Unternehmens genau

CyberXperts hilft Ihnen dabei, aktuelle Gefahren zu identifizieren und geeignete Gegenmaßnahmen umzusetzen. So haben Angreifer bei Ihrem Unternehmen keine Chance!

Mit dem CyberXperts-Dashboard sehen Sie alle Risiken auf einem Blick. Mit ausgewählten Fragen analysieren wir Ihr Risikoprofil und zeigen mögliche Szenarien.

Verständliche Schritt-für-Schritt-Maßnahmen

Sie erhalten zu jeder potenziellen Bedrohung individuelle Maßnahmen, um Ihr Unternehmen besser zu schützen. Mit einer leicht verständlichen Schritt-für-Schritt-Anleitung können Sie diese kinderleicht in Ihrem Unternehmen umsetzen.

Immer im Blick und automatische Erinnerungen

Damit Ihre IT-Sicherheit im Alltagsstress nicht in Vergessenheit gerät, erinnern wir Sie rechtzeitig daran und analysieren die aktuelle Sicherheitslage Ihres Unternehmens.

Ja, ich möchte mehr über den 360°-Check für mein Unternehmen erfahren.

Wir freuen schon auf Ihre Terminvereinbarung!

Impressum

CyberXperts

ein Unternehmensbereich der
VNR Verlag für die Deutsche Wirtschaft AG
Theodor-Heuss-Straße 2-4; D-53095 Bonn

Vorstand: Richard Rentrop

Telefon: 0228 - 9 55 01 60 (Kundendienst)
Telefax: 0228 - 3 69 64 80
E-Mail: info@cyberxperts.de
Internet: https://www.cyberxperts.de

Verantwortlicher i.S.d.P.: Michael Jodda, Theodor-Heuss-Straße 2-4, 53177 Bonn

Enthält u. a. Artikel von Andreas Hessel, Andreas Würtz, Olaf Reuter

Satz: BB-Design, Birken-Honigsessen

Bildnachweis: S. 1 WhataWin, S. 7 Olivier Le Moal, S.9 fitzkes, S. 10 Alexander Limbach, S. 11 IconWeb, S. 13 ronnarong, S. 14 Jose, S. 18 U-STUDIOGRAPHY DD59, S. 22 und 30 NicoElNino, – alle Adobe-Stock; S. Grafiken auf S. 38 und 39 – CyberXperts.

Bonn, Berlin, Bukarest, Jacksonville, Manchester, Warschau