

B E R N H A R D

ASSEKURANZMAKLER

SEIT 1950



EINFACH. VERTRAUENSVOLL. VERSICHERT.

Das Whitepaper zum Thema Cyberschutz für Vereine und Verbände

Das Whitepaper zum Thema Cyberschutz für Vereine & Verbände

Immer wieder hört man von Cyber-Angriffen auf große Unternehmen. Der Angriff auf das Internetunternehmen Yahoo im September 2016 zählt noch heute zu dem größten Hacker-Angriff aller Zeiten. Damals wurden knapp eine Milliarde Namen, Adressen und Passwörter von den Usern gestohlen, wovon sich das Unternehmen nur schwer erholte.

Doch auch mittelständische Betriebe sind häufig betroffen, denn heutzutage gibt es kaum jemanden mehr, der seine Daten nicht digital verwaltet. Die Cyber-Versicherung kann hier den nötigen Rückhalt bieten.

In den meisten Unternehmen ist das reibungslose Funktionieren der IT für die Geschäftsabläufe essentiell.

Gerade die digitale Vernetzung untereinander bringt viele Vorteile mit sich. Im Falle eines Cyber-Angriffs kann aber genau das zum Verhängnis werden: im schlimmsten Fall muss der laufende Betrieb sogar komplett unterbrochen werden, was existenzielle Folgen mit sich bringen kann. Dieser Eigenschaden kann durch die richtige Cyber-Versicherung vollständig abgedeckt werden.

Cyber-Kriminalität kann aber nicht nur Eigenschäden verursachen, sondern sich schnell auch gegen Dritte, wie zum Beispiel Ihre Kunden oder Geschäftspartner, wenden. Durch den Verlust von wichtigen Daten verlieren Sie möglicherweise das Vertrauen Ihrer Kunden. Auch diese Art von Schaden kann schnell existenzgefährdend werden. Deshalb ist ein umfassendes Cyber-Schutzkonzept unverzichtbar.

Vereine & Verbände



Die Cyberversicherung - Was sie kann und für wen sie sinnvoll ist

1. Welche Gefahren deckt eine Cyber-Versicherung ab?.....	4
2. Warum genügt eine normale Haftpflichtversicherung nicht?.....	5
3. Für welche Vereine und Verbände ist eine Cyber-Versicherung sinnvoll?.....	6
4. Die verschiedenen Arten von Cyber-Angriffen.....	7
5. Die sechs Phasen eines Cyber-Angriffs und wie man sie verhindern kann.....	8
6. Schutzmaßnahmen.....	11
7. Wie verhalte ich mich im Falle eines Cyber-Angriffs richtig?.....	12
8. Fünf wertvolle Tipps zum Schluss.....	13
9. Fazit & Kontakt.....	14
10. Das Cyberkonzept der Bernhard Assekuranz für Ihre Organisation.....	14
11. FAQs zum Thema Cyberschutz.....	15

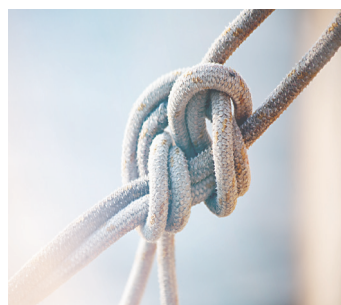


Welche Gefahren deckt eine Cyberversicherung ab?

Die Cyber-Versicherung kommt finanziell für zahlreiche mögliche Schäden, die Ihrem Verein oder Verband zugefügt wurden, auf. Darüber hinaus werden Sie von erfahrenem IT-Experten bei der (PR-) Krisenbewältigung unterstützt und betreut. Außerdem erhalten Sie Hilfe bei der Wiederherstellung Ihrer Daten. Auch eventuell anfallende Rechtsverfolgungs- und Sachverständigenkosten übernimmt die Cyber-Versicherung.

DIE WICHTIGSTEN BESTANDTEILE AUF EINEN BLICK

- › Datenverlust, Zerstörung oder Beschädigung
(mutwillig oder durch menschliches Versagen zustande gekommen)
- › Betriebsunterbrechung oder Beeinträchtigung
in der betrieblichen Leistungserstellung
- › Online-Erpressung - Erpresser fordern Geld,
ansonsten zerstören sie die Daten vollständig oder geben sie frei
- › Folgekosten -
Software-Wiederherstellung oder Kosten für die Sachverständigung
- › Schadenersatzansprüche - Ansprüche Dritter aufgrund einer
Datenschutzverletzung
- › Telefon-Hacking - über das gehackte Telefon wurde eine
hohe Telefonrechnung erzeugt
- › Computerbetrug im Sinne eines vorsätzlichen, rechtswidrigen und ziel-
gerichteten Angriffs eines Dritten über das Internet in betrügerischer Absicht





VEREINE & VERBÄNDE

Warum genügt eine normale Haftpflicht nicht?

Bei der klassischen Vereinshaftpflichtversicherung sind die Risiken, die eine Cyberversicherung zusätzlich abdeckt, nicht mit inbegriffen.

Hierzu zählt unter anderem die Unterstützung bei der Krisen-PR oder bei der Wiederherstellung der Daten. Außerdem sind bei der Cyberversicherung, im Gegensatz zur „normalen“ Haftpflicht auch Eigenschäden mitversichert.

Für welche Vereine & Verbände ist eine Cyberversicherung sinnvoll?

Verbände, die eine große Zahl von personenbezogenen Daten verwalten oder allgemein einen hohen digitalen Vernetzungsgrad aufweisen, sind ein beliebtes Ziel von Hacker-Angriffen. Abhängig von der Größe hat jeder Verein oder Verband seinen eigenen Risikobedarf, den es zu ermitteln gilt, um den optimalen Versicherungsschutz zu gewährleisten.

Wie Sie also feststellen konnten, kann ein Cyber-Angriff tendenziell jeden treffen. Wenn Sie über den Abschluss eines Cyber-Schutz-Paketes nachdenken, sollten Sie sich darüber im Klaren sein, dass eine Versicherung vor allem immer dann Sinn macht, wenn der potentielle Schaden große bis existentielle Ausmaße annehmen und so das Bestehen Ihrer Organisation gefährden kann.

Darüber hinaus sollte jeder Verein oder Verband für sich prüfen, ob die technischen Schutzmaßnahmen dem empfohlenen Mindestmaß entsprechen und hier gegebenenfalls nachrüsten.

Es empfiehlt sich zudem, einen Notfallplan zu erstellen, der im Krisenfall alle notwendigen Schritte beschreibt, die nötig sind, um sämtliche Systeme wiederherzustellen. Wem das nicht ausreicht und wer sich stattdessen noch umfassenderen Schutz wünscht, sollte die Cyberversicherung unbedingt in Betracht ziehen.

In diesem Zusammenhang sollten Sie folgende Fragen grundlegend für sich beantworten:

Welches Risiko besteht?

Wie hoch könnte der Schaden im schlimmsten Fall sein?

Können Sie im Falle eines Angriffs die Kosten für Krisenmanagement, IT-Rechtsberatung und Reputations- und Reparationsmanagement selber tragen?

Können Sie 100%ig ausschließen, dass Sie einen Datenträger (Laptop) oder vertrauliche Daten (Kundeninformationen und Passwörter) niemals verlieren?



Die verschiedenen Arten von Cyberangriffen

Es gibt unzählig viele Situationen, in denen Sie die Opfer eines Hacker-Angriffs werden können. Eine kleine Auswahl dieser zeigt, gegen was Sie sich in einem solchen Fall durch eine Cyberversicherung schützen können.

Die ungezielten Online-Attacken

Maleware - z.B. Viren, Trojaner

CryptoLocker - verschlüsselt die Daten auf einem Computer vollständig, sodass Sie keinen Zugriff mehr darauf haben

Veränderungen an IT- oder Betriebssystemen - Beeinträchtigung der Computersicherheit

Fehlfunktion durch Manipulation

Die gezielten Online-Attacken

Hacker-Angriff - z. B. Diebstahl sensibler Daten oder Manipulation der Verbands- oder Vereinswebsite

„Denial of Service“-Angriff, kurz DOS-Angriff - Computer und Server sind nicht mehr erreichbar

Phishing - mit Hilfe von gefälschten E-Mails oder Websites stehlen Cyber-Kriminelle Passwörter und andere sensible Daten

Beispiel: „Fake President“ - Buchhaltung bekommt eine gefälschte Email von dem Email-Account des Geschäftsführers, mit der Aufforderung einen Betrag von 20.000€ zu überweisen

Missbrauch der Identität - unbefugte Aktivitäten z. B. bei Online-Banking





VEREINE & VERBÄNDE

Die sechs Phasen eines Cyber-Angriffs und wie man sie verhindern kann

Ist der Eindringling erst einmal im System, gestaltet es sich als äußerst schwierig, ihn wieder los zu werden. Besser ist es gar nicht erst so weit kommen zu lassen. Mit einigen wenigen Handgriffen können Sie vorsorgen und so einen Cyber-Angriff gar nicht erst zustande kommen lassen.

PHASE 1: DAS AUSSPIONIEREN

Durch Spionage-Phishing Taktiken oder das Ausspionieren von Social-Media Profilen der Mitarbeiter verschafft sich der Internet-Kriminelle einen ersten Überblick. Die gesammelten Daten verwendet er dann, um gezielte Nachrichten und Anfragen zu verschicken, die die Mitarbeiter dazu bringen, auf einen risikoreichen Link zu klicken oder infizierte Anhänge zu öffnen. Die dadurch heruntergeladene Malware wird von den Hackern dazu verwendet, um aktiv nach Schwachstellen zu suchen.

Wie Sie das verhindern können

Zu aller erst schulen Sie Ihre Mitarbeiter. Machen Sie ihnen klar, dass sie auf keinen Fall unautorisierte Mails öffnen sollen. Sollte einem Mitarbeiter darüber hinaus etwas Verdächtiges aufgefallen sein, muss er sich umgehend an das dafür zuständige Team wenden und auch andere Mitarbeiter warnen. Verwenden Sie sogenannte URL-Filter. Diese hindern den Angreifer daran, Social-Media- und Websiteinformationen zu manipulieren. Außerdem können Sie den Netzwerkverkehrsfluss mit Hilfe von Intrusion-Prevention-Technologien absichern, um eine Bedrohung rechtzeitig zu erkennen.

PHASE 2: DIE VORBEREITUNG

Cyber-Kriminelle kennen eine Vielzahl von Methoden, um in das System einzudringen. Ein gängiges Vorgehen ist hier beispielsweise die Einbettung von Intruder-Codes in Dateien und E-Mails.

Wie Sie das verhindern können

Sie haben die Möglichkeit, diesen Zyklus mit Hilfe einer Firewall zu durchbrechen. Diese ermächtigt Ihnen Einblicke in den gesamten Datenverkehr und blockiert Risiko-Anwendungen.



VEREINE & VERBÄNDE

Die sechs Phasen eines Cyber-Angriffs und wie man sie verhindern kann

PHASE 3: DIE AUSBEUTUNG

Nachdem der Hacker den Zugriff auf das Netzwerk erlangt hat, kann er nun einen Code aktivieren, um bestimmte Ziele unter seine Kontrolle zu bringen.

Wie Sie das verhindern können

Generieren Sie einen sogenannten Endpunktschutz, um bekannten aber auch unbekanntesten Schwachstellen-Exploits den Zugang zu verhindern. Exploits zeigen dem Hacker Sicherheitslücken der Software auf und helfen ihm, diese auszunutzen.

PHASE 4: DIE INSTALLATION

Der Internet-Kriminelle richtet nun verschiedene Systeme in dem Netzwerk ein. Hierzu zählt unter anderem der sogenannte Rootkit. Das ist eine Sammlung von verschiedenen Software-Werkzeugen, die auf dem betroffenen System installiert werden, um Anmeldevorgänge des Hackers zu verbergen. So kann er unbemerkt seinen Schaden anrichten.

Wie Sie das verhindern können

Hier helfen ebenfalls die Endpunktschutz-Technologien.

PHASE 5: DIE KONTROLLE

Nun richtet der Angreifer einen Rückkanal zum Server ein. So können Daten zwischen infizierten Geräten und dem Server unbemerkt ausgetauscht werden und so eine baldige Infizierung des gesamten Systems hervorrufen.

Wie Sie das verhindern können

Durch sogenannte Anti CnC-Signaturen können ausgehende Anweisungen an den Server blockiert werden. Die URL-Filterung verhindert zusätzlich eine Kommunikation mit risikoreichen URLs.



VEREINE & VERBÄNDE

Die sechs Phasen eines Cyber-Angriffs und wie man sie verhindern kann

PHASE 6: DIE MANIPULATION

Konnte sich der Angreifer durch jegliche Sicherheitsbarrieren des Netzwerkes durchkämpfen, beginnt er nun, das System für seine Zwecke zu missbrauchen. Dies äußert sich in den meisten Fällen durch den Klau von Daten, eine mutwillige Zerstörung dieser oder eine Erpressung des Unternehmens.

Wie Sie das verhindern können

Es gibt die Möglichkeit, die Freiheit, mit der sich der Hacker im System bewegt, durch Datei-Übertragungsrichtlinien einzuschränken. Ist man allerdings an diesem Punkt angelangt, gibt es kaum eine Möglichkeit der aktiven Schadensbekämpfung. Nun gilt es viel mehr, den aufkommenden Schaden so gering wie möglich zu halten.

Trotz aller Vorsichtsmaßnahmen kann das Durchdringen eines Cyber-Angriffs niemals vollständig verhindert werden. Da die Kosten eines solchen Angriffs existenzgefährdend sein können, ist der Schutz durch eine Versicherung, die all diese Risiken absichert, eine lohnenswerte Investition. Gerade Unternehmen, die fast alle Arbeitsabläufe über ihre IT regeln, sollten diesen Risikofaktor aus dem Weg schaffen.

Schutzmaßnahmen

1. Line of Defence – Außenwirkung

Schutzschild

- Effektive Firewalls
- Moderne Serverlandschaften
- Regelmäßige Installation aktueller Patches/Updates

2. Line of Defence – Innenwirkung

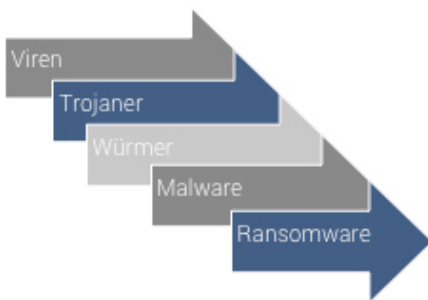
Strukturen, Prozesse, Verständnis

- Sensibilisierung der Mitarbeiter
- Cyber-Risk-Governance
- Berücksichtigung von Cyber-Gefahren in die Wertschöpfungskette

3. Line of Defence – Restrisikowirkung

Cyber-Versicherung

- Umfassende Deckung
- Umfassende Serviceleistung
- Solider, starker Versicherer



Mit Hilfe des Einbaus von Viren, Trojanern, Würmern, Malware oder Ransomware kann ein Angreifer sich unberechtigten Zugriff auf Ihre Systeme und Ihr Netzwerk verschaffen. Ransomware ist eine Art von Malware, die Daten kidnappt. Der Angreifer verschlüsselt die Daten der Opfer und verlangt ein Lösegeld für den privaten Schlüssel. Im ersten Schritt der Abwehr sollten Sie also effektive Firewalls installieren, moderne Serverlandschaften einrichten und regelmäßige Installationen aktueller Patches und Updates durchführen.

Im zweiten Schritt der Abwehr ist es wichtig, innere Strukturen und Prozesse auf Cyberschutz auszurichten um ein Verständnis für die Gefahr zu schaffen. Dazu gehört vor allem die Sensibilisierung der Mitarbeiter für das Thema. Weiterhin sollte die Führungsebene dafür Sorge tragen, dass die für den Cyberbereich geltenden Vorschriften ordnungsgemäß eingehalten und umgesetzt werden, um den Anspruchs- und Haftungsfallen möglichst zu entgehen.

Trotz aller Vorsichtsmaßnahmen besteht ein gewisses Restrisiko. An dieser Stelle kann Ihnen die Cyberversicherung zusätzliche Absicherung gewährleisten. Die Cyberversicherung bietet eine umfassende Deckung, sowie Serviceleistungen. Zudem steht Ihnen mit der Bernhard Assekuranz ein solider und starker Partner, der auf über 65 Jahre Erfahrung zurückblicken kann, zur Seite.








KRISENPLAN

Wie verhalte ich mich im Falle eines Cyber-Angriffs richtig?

Trotz Ihrer getätigten Schutzmaßnahmen wird Ihr Verein oder Verband Opfer eines Cyber-Angriffs? Hier sind die wichtigsten Punkte, auf die Sie nun achten sollten:

KRISENPLAN



-  1 Bewahren Sie Ruhe!
-  2 Verschaffen Sie sich einen Überblick über die Lage!
-  3 Rufen Sie die Krisenhotline Ihres Versicherers an!
-  4 Benutzen Sie die Systeme nicht weiter und schalten Sie sie auch nicht aus!
-  5 Tätigen Sie keine Zahlungen!

Fünf wertvolle Tipps zum Schluss

1. Beauftragen Sie ein Einsatzteam, das im Krisenfall als erster Ansprechpartner fungiert und für alle wichtigen Schritte, wie z.B. die Kontaktaufnahme mit der Versicherung, zuständig ist.

2. Entwickeln Sie eine Sicherheitsstrategie.

3. Installieren Sie regelmäßig alle neuen System-Updates, um sich bestmöglich vor einem Cyber-Angriff zu schützen.

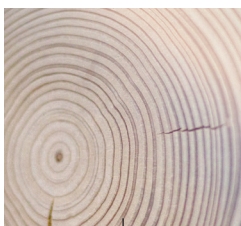
4. Beziehen Sie auch den Vorstand mit ein. Machen Sie ihm klar, wie wichtig der Schutz vor Cyber-Angriffen ist und halten Sie ihn auf dem Laufenden, um sich vor allem eine ausreichende, auch finanzielle Unterstützung zu sichern.

5. Erstellen Sie mindestens eine Sicherheitskopie aller Daten, damit so viele Dateien wie möglich auch nach einem Datenverlust wiederhergestellt werden können.

Hier noch ein kleiner Exkurs zum Thema fake president - Mails:

Erhöhte Aufmerksamkeit gilt bei sogenannten „fake president“-Mails, die angeblich von der Geschäftsleitung kommen, und in denen eine Überweisung angewiesen wird. Das gilt v.a. bei Überweisungen an eine Bank im Ausland und ohne Bezug zu einem bekannten Vorgang. Bei solchen Mails ist die Angelegenheit unbedingt nochmal telefonisch mit dem jeweiligen Verantwortlichen zu verifizieren. Hinterlegen Sie bei Ihrer Bank, dass Überweisungsträger und Auslandsüberweisungen immer telefonisch zu bestätigen sind - insbesondere, wenn Sie Online-Banking vereinbart haben. Auch sollten Sie ein vier Augen-Prinzip bei Überweisungen einführen und Ihre Mitarbeiter unbedingt um Aufmerksamkeit bitten.

Lieber einmal zu viel fragen, als auch nur einmal zu wenig.



INDIVIDUELL



VERLÄSSLICH



OBJEKTIV



SICHERHEIT

Fazit & Kontakt

Wir befinden uns im digitalen Zeitalter. Schon jetzt ist die IT nicht mehr aus unserem Alltag wegzudenken. Ähnlich geht es auch gemeinnützigen Organisationen: viele Prozesse und Arbeitsabläufe lassen sich heutzutage bequem per Mausklick erledigen.

Damit das auch so bleibt, sollte jeder Verein oder Verband, früher oder später über eine Cyber-Versicherung nachdenken. Sie abzuschließen ist einfach und mit den verschiedenen Bausteinen lässt sich ein Versicherungspaket nach Ihren individuellen Bedürfnissen zusammenstellen. Sichern Sie sich also rechtzeitig gegen die finanziellen und image-schädigenden Risiken eines Cyber-Angriffs ab.



SICHERHEIT

Das Cyber-Konzept der Bernhard Assekuranz für Ihre Organisation

Die Bernhard Assekuranz ist seit über 60 Jahren spezialisiert auf gemeinnützige Einrichtungen. Wir kennen Ihr Risiko und Ihre Bedürfnisse. Zu unseren Kunden zählen circa 14.000 gemeinnützigen Einrichtungen. Wir bündeln Ihre Interessen und machen uns dafür bei den Versicherern stark.

Um Ihre Organisation vor den finanziellen Folgen aus Cyber-Risiken zu schützen, haben wir speziell für gemeinnützige Einrichtungen (Vereine, Verbände, gGmbHs) ein Sonderkonzept zum Cyber-Schutz erarbeitet.

Unser Cyber-Konzept zeichnet sich dadurch aus, dass es sich an den spezifischen Risiken und Bedürfnissen der gemeinnützigen Einrichtungen orientiert.

Nutzen Sie diese Chance und versichern Sie sich über uns.

Wir bieten Ihnen ein bedarfsgerechtes Deckungs-Konzept zu einem fairen Preis. Rechtliche Informationen finden Sie unter:

<https://bernhard-assekuranz.com/rechtliche-informationen/>

Bernhard Assekuranzmakler GmbH

SICHERHEIT



FAQs zum Thema Cyberschutz



Clickjacking

Der Inhalt einer Website wird mit unsichtbaren Bestandteilen einer anderen Website überlagert. Dies kann z.B. dazu führen, dass das Opfer unwissentlich Zugriff auf Webcams und Mikrofone genehmigt.

(D)DoS Attacke

Das IT-System des Opfers wird mit einer Vielzahl von Anfragen bombardiert, um das Computersystem des Opfers zu überlasten und dessen Verfügbarkeit anschließend außer Kraft zu setzen. Eine Betriebsunterbrechung ist meist die Folge.

Datensicherung

Auch Backup genannt. Das Kopieren von Daten auf einem separaten oder externen Speicher in der Absicht, diese Daten im Fall eines Datenverlustes zurückkopieren zu können.

Datenverschlüsselung

Zweck ist die Gewährleistung der Vertraulichkeit von Daten bzw. Verhinderung des Missbrauchs von Daten durch Unbefugte durch die Umwandlung von Daten (Klartext) in eine andere sinnlos erscheinende Ansammlung von Informationen (Geheimtext). Dieser Schutz basiert auf einer speziellen Verknüpfung der Daten mit einem sogenannten Schlüssel.

Hacktivismus

Ist die Verwendung von Computern und Netzwerken als Protestmittel.

Hacker

Ein Computerspezialist, der einen Quellcode schreiben oder verändern kann. Hacker oder auch Cracker handeln aus kriminellen Motiven, um einen größtmöglichen Schaden durch Vandalismus im Computersystems des Opfers zu verursachen und/oder Daten zu stehlen und zu missbrauchen.

Firewall

Zweck ist die Sicherung/Schutz (Software) des Computersystems vor unerwünschten Zugriffen Dritter. Die Firewall an jedem Internetport (Zugang des Computersystems des VN in das Internet) des Computersystems des VN ist eine Art „Grenzübergang“, an dem die in das Computersystem eintretenden Daten nach vorgegebenen Regeln geprüft werden. Firewall-Software beschränkt den Netzwerkzugriff, überwacht den laufenden Datenverkehr und entscheidet anhand bestimmter Regeln, ob Netzwerkpakete zugelassen werden.



FAQs zum Thema Cyberschutz



IT-Sicherheit

IT-Sicherheit bezeichnet den Schutz von Computersystemen (Software und Hardware) und deren Werte (Daten) vor etwaigen Bedrohungen. Zudem sollen mit ihrer Unterstützung wirtschaftliche Schäden verhindert werden.

Mailbombe

Beschreibt das organisierte Verschicken einer Vielzahl von Mails, um die Kommunikation des Empfängers zu blockieren. Eine Betriebsunterbrechung ist oft die Folge.

Malware

Schadprogramme, die unerwünschte schädliche Funktionen im Computersystems des Opfers ausführen, wie z.B. Manipulation oder Löschen von Daten.

Personenbezogene oder sonstige sensible Daten

Daten, aus denen die rassistische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie die Verarbeitung von genetischen oder biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (Definition nach Art 9 DSGVO).

Regelmäßige Updates

in konstanten zeitlichen Abständen wiederkehrende Aktualisierung von Software oder Daten.

Schadsoftware

Software, die unberechtigt oder ungewollt in Computersysteme eingeschleust werden und dessen Software schädigen kann, z.B. durch Veränderung, Löschung und Blockaden.

Server

Auch Hostrechner genannt. Er stellt Computerfunktionen und Ressourcen (Arbeitsspeicher, Anwendungsprogramme) zur Verfügung, auf die andere Computer zugreifen können.

Spear Phishing

Sind gefälschte Mails oder Websites, deren Ziel es ist, an persönliche Daten, wie z.B. Passwörter oder Login-Daten des Nutzers zu gelangen. Folge ist z.B. Kontoplünderung.



FAQs zum Thema Cyberschutz



„Stand der Technik“

Ein gängiger juristischer Begriff, der nicht allgemeingültig und abschließend definiert ist (unbestimmter Rechtsbegriff).

Da die technische Entwicklung schneller voranschreitet, als die Gesetzgebung, hat es sich bewährt, in Gesetzen den Begriff „Stand der Technik“ zu verwenden, statt zu versuchen, konkrete technische Anforderungen festzulegen. Was zu einem bestimmten Zeitpunkt „Stand der Technik“ ist, lässt sich zum Beispiel anhand existierender nationaler oder internationaler Standards und anhand erfolgreich in der Praxis erprobter Vorbilder für den jeweiligen Bereich ermitteln.

(Quelle: Bundesamt für Sicherheit in der Informationstechnik, BSI)

Stand der Technik ist daher nicht gleichzusetzen mit „stets neueste und aktuellste“ Technik, sondern eine Technik, die nach den Standards noch als angemessen und aktuell angesehen wird. Entscheidend ist also eine Verhältnismäßigkeit der Maßnahmen zu drohenden Schäden. Auch ein älteres Computersystem kann somit auf dem Stand der Technik sein, solange die Software entsprechend aktuell ist. Die Basis dazu wird durch die Fragen im Risikofragebogen beschrieben, z.B:

- jeweils aktuelle Firewall, Virens Scanner, Datenverschlüsselung, Datensicherungen
- verbindliche Regelungen zu Umgang mit Schadsoftware; Datensicherung, Nutzung der IT, Zugriffsberechtigungen (Administratorenrechte), regelmäßige Updates (Patch-Management)



Es ist jedoch möglich, dass sich neue Sicherheitsrisiken ergeben, welche neue Reaktionen erfordern, die nicht abgefragt werden, aber dennoch zum Stand der Technik gehören können. Letztlich ist dies der Schnellebigkeit und rasanten technischen Entwicklung geschuldet, die es erfordert, die IT-Systeme aktuell zu halten, um den Wettlauf gegen Angreifer nicht zu verlieren. Diese Verantwortung liegt bei dem IT-Nutzer und kann vom Versicherer nicht vollständig übernommen werden.

Auch in anderen Bereichen, z.B. Brandschutz, ist es üblich, dass der Nutzer eines Gebäudes für die technische Sicherheit verantwortlich ist. Kommt es dennoch zu Schäden, sind diese versicherbar. Nicht abgedeckt werden können jedoch solche Risiken, die durch eine mangelhafte technische Aktualität überhaupt erst möglich werden.

Die Verpflichtung, die IT-Systeme auf dem Stand der Technik zu halten ermöglicht es erst, die Risiken abzusichern. Werden die genannten Basisanforderungen eingehalten, also vor allem die Software durch updates und patches aktuell gehalten, so wird der Stand der Technik in der Regel gewährleistet sein.

FAQs zum Thema Cyberschutz



Trojaner

Schadprogramm, das ohne Wissen des Anwenders Daten ausliest. Die Folge ist meist die Veränderung, der Verlust und/ oder die Unbrauchbarkeit von Daten.

Verbindliche Regelung

verpflichtende bzw. bindende Vereinbarung, ein bestimmtes festgelegtes Verhalten zu verwirklichen. Regelung ist die Erklärung oder Beschreibung des verpflichtend festgelegten Verhaltens, z.B. schriftliche Datenschutzrichtlinien eines Betriebes für Mitarbeiter, Datenschutzvereinbarungen als Betriebsvereinbarungen eines Unternehmens, Anweisung des Arbeitgebers (oder dessen Vertreters) zum Umgang mit Daten zu deren Schutz gegenüber den Mitarbeitern.

Virens Scanner

Zweck ist das Erkennen und Beseitigen von Schadprogrammen in der Software. Die im Computersystem des VN bekannte (durch Virensignatur erkennbare) Computerviren, Computerwürmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt.

Aktuelle Virensignatur

Die Merkmale (Regelmäßigkeiten des Virencodes/DNA) eines Virus werden erfasst und zusammengestellt, um einen Virus im IT-System/Betriebssystem, Anwendungsprogrammen des Computersystems zu erkennen und zu identifizieren.

Virus

Verbreitungs- oder Infektionsvirus, der sich im System des Opfers selbst reproduziert wird in Computersysteme eingeschleust und kann zu Veränderungen am Betriebssystem, an Software oder auch Hardware führen. Die Verbreitung findet durch Wechselmedien wie Web-Server, FTP-Server, Tauschbörsen oder Social Media statt. Die Veränderung, der Verlust und die Unbrauchbarkeit von Daten sind oft die Folge.

Wurm

Schadprogramm, das aktiv oft über Netzwerke und Wechselmedien verbreitet wird und sich in andere Programmdateien einfügen kann. Meist wird ein Hilfsprogramm oder eine Anwendungssoftware verwendet, um im Computersystem des Opfers zu starten. Es wird ein erhöhter Verbrauch von Ressourcen generiert, welcher so zum Ausfall von Netzwerkteilnehmern (z.B. Flughafen Wien-Schwechat - Totalausfall - BU- durch den Wurm Sasser) führt. Die Folge ist meist die Veränderung, der Verlust und die Unbrauchbarkeit von Daten und auch Überlastung des Computersystems des Opfers bis zur Betriebsunterbrechung.

Zugriffsberechtigung

Rechte, die einem Anwender bzw. Benutzer in einem Netzwerk, im Internet oder einem ähnlichen Kommunikationssystem durch den Systemverantwortlichen bzw. Systemadministrator eingeräumt werden.

