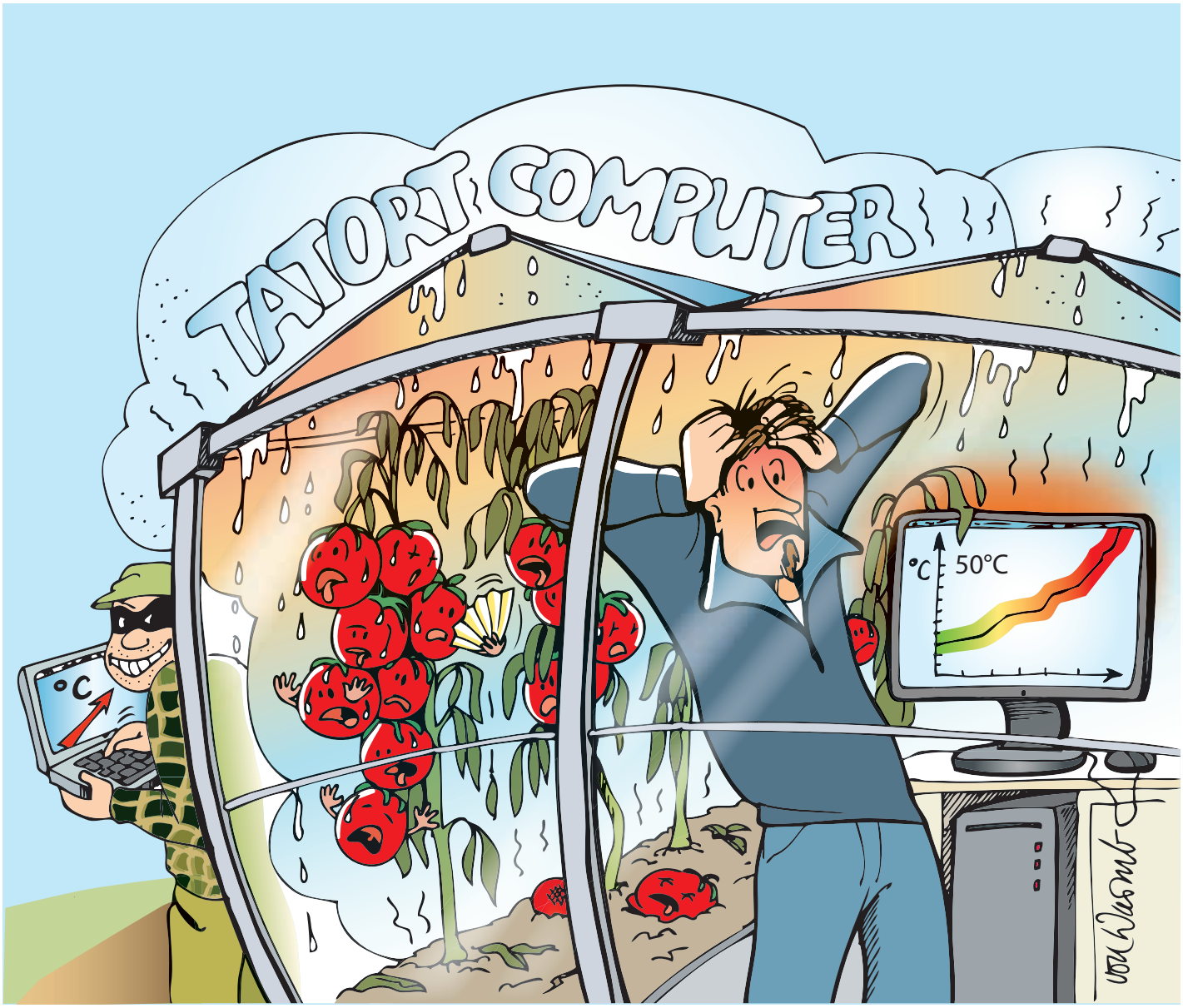
BEITRÄGE ZUR BETRIEBSSICHERHEIT

33



Cyberschutz im Gartenbau

- Cyberkriminalität und Gefahrenpotenzial
- Folgen erfolgreicher Cyberangriffe
- Maßnahmen zur Schadenverhütung, -minimierung

www.GeVau.de

GARTENBAU VERSICHERUNG
Gärtner versichern Gärtner.

Cyberschutz betrifft jeden

Stellen Sie sich vor, es ist Hochsaison und in Ihrem Gartenbaubetrieb werden die Computer hochgefahren. Es erscheint eine Anzeige, die Sie darüber informiert, dass Ihre Daten verschlüsselt wurden. Die einzige Möglichkeit, wieder Zugriff auf Ihre Daten zu erlangen bestehe darin, einen Code zu erwerben, mit dessen Hilfe diese Sperre aufgehoben werden kann. Alle Arbeiten, die durch die Nutzung von Computern einfach und schnell erledigt werden, sind nur noch per Hand oder nicht mehr ausführbar.

Hätten Sie gewusst, dass ein solches Szenario schon dadurch ausgelöst werden kann, dass Sie einen E-Mail-Anhang eines „Bewerbers“ arglos geöffnet und auf Nachfrage des Computers dessen Bearbeitung zugelassen haben?

Wenn Sie diese Frage verneinen, sollten Sie sich dringend mit dem Thema Cyberschutz auseinandersetzen!

Das beschriebene Szenario kann jedem widerfahren, der mit dem Internet verbundene Server, Computer, Tablets, Smartphones oder sonstige Endgeräte nutzt. Zusammengenommen bilden diese umgangssprachlich den **Cyberspace**. Wenn dies geschieht, wurden Sie Opfer einer netzbezogenen Straftat, was allgemein als **Cybercrime** bezeichnet wird. **Cyberschutz** ist in der heutigen Zeit für nahezu jeden von Bedeutung. Dies ergibt sich aus der repräsentativen Umfrage „Cyberrisiken im Mittelstand 2018“, die von der Forsa im Auftrag des Gesamtverbandes der Deutschen Versicherungswirtschaft (GDV) durchgeführt wurde. Demnach waren 30 % der befragten 300 kleinen und mittleren Unternehmen Opfer erfolgreicher Cyberangriffe (Abb. 1, S. 2). Alle in diesem Beitrag zur Betriebssicherheit aufgeführten Statistiken, die als Quelle mit „GDV“ gekennzeichnet sind, stammen aus dieser Umfrage.

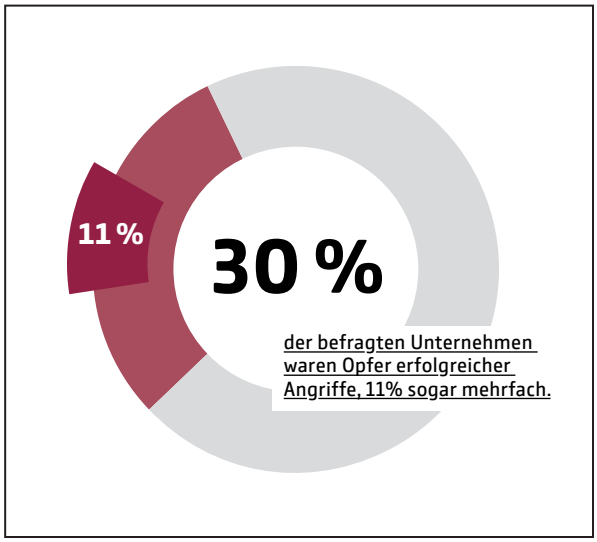


Abb. 1: Anteil an Unternehmen, die bereits durch einen Cyberangriff geschädigt wurden (Quelle: GDV, siehe S. 12)

Was bedeutet Cyber?

Laut Duden handelt es sich bei dem Wort „Cyber“ um ein Wortbildungselement mit der Bedeutung „die von Computern erzeugte virtuelle Scheinwelt betreffend“. Cyberspace beziehungsweise -raum meint also im allgemeinen Sprachgebrauch „das Internet“, das sich aus der Vernetzung aller beteiligten Computer ergibt. Cyberkriminalität oder Cybercrime nennt man alle kriminellen Tätigkeiten, die im, am oder durch den Cyberspace verübt werden. Cyberschutz bezeichnet demnach alle Maßnahmen, die dem Schutz des Cyberspace dienen.

Abb. 2: Sperrbildschirm eines mit der Schadsoftware „WannaCry“ betroffenen Computers

Das am Anfang beschriebene Schadenereignis hätte durch das Einhalten einfacher Sicherheitsmaßnahmen unwahrscheinlich gemacht oder verhindert werden können. Insbesondere für Betriebsleiter ist es wichtig, sich mit diesen Themen auseinanderzusetzen, da durch einen erfolgreichen Cyberangriff große betriebswirtschaftliche Schäden entstehen können. Der vorliegende Beitrag zur Betriebssicherheit soll hel-

fen, das vorhandene Gefahrenpotential einzuschätzen sowie mögliche präventive und akute Maßnahmen, die man als Cyberschutz zusammenfassen kann, aufzuzeigen.

Gefahrenpotential

Durch Computerbetrug, Ausspähen von Daten, Computersabotage und weitere Delikte entstehen alleine in Deutschland laut Bundeskriminalamt (BKA) Schäden in Höhe von mehr als 39 Millionen Euro jährlich – Tendenz steigend. Fast 50.000 Straftaten aus dem Bereich Cybercrime schlugen sich im Jahr 2015 in der Kriminalstatistik des BKA nieder (Abb.3, S. 3). Die Dunkelziffer wird deutlich höher geschätzt. Gesetzesänderungen erhöhen zunehmend den Druck auf Unternehmen, ihre IT-Sicherheit zu verbessern. Die Unternehmenssicherheit mit ihren klassischen Handlungsfeldern Brandschutz, Naturgefahren (Hagel, Sturm, Überschwemmung, Starkregen usw.) und Sicherheit (Schutz gegen Einbruch, Diebstahl, Sabotage) muss heute um den Aspekt „Cyberschutz“ ergänzt werden.

Angriffe aus dem Internet, sogenannte „Cyberattacken“, können jeden treffen. Manche Schadsoftware betrifft zehntausende Endgeräte. Im Mai des Jahres 2017 ereignete sich der bisher größte bekannte Cyberangriff durch die Schadsoftware WannaCry. Es wurden Daten auf 230.000 Computern in 150 Ländern verschlüsselt, die erst nach Zahlung eines Lösegelds wieder zugreifbar sein sollten (Abb. 2, S. 1). In diesem speziellen Fall war die Zahlungsfunktion fehlerhaft und die Daten konnten selbst nach Zahlung des Lösegelds nicht wiederhergestellt werden. Die Schadsoftware nutzte eine Sicherheitslücke von älteren Microsoft Windows-Versionen. Betroffen waren unter anderem Computer der Deutschen Bahn, was dazu führte,

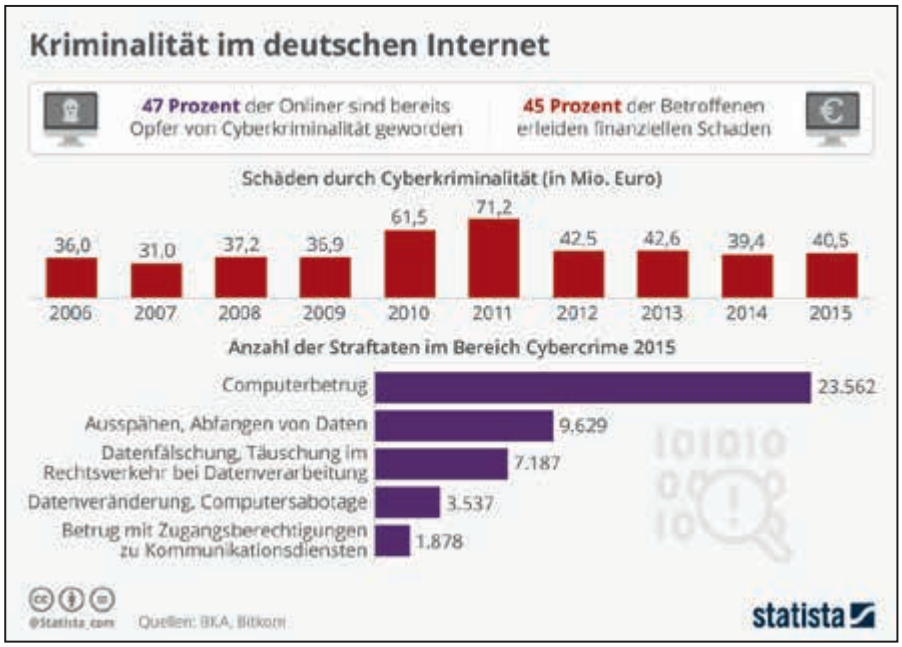


Abb. 3: Schäden durch Cyberkriminalität in Deutschland in Mio. Euro und Anzahl der Straftaten im Bereich Cybercrime im Jahr 2015 (Quelle: Statista)

dass die Erpressungsnachricht in manchen Bahnhöfen öffentlich und medienwirksam auf Anzeigetafeln sichtbar wurde.

Dies ist insbesondere vor dem Hintergrund beachtlich, da bereits Mitte März desselben Jahres von Microsoft ein Update bereitgestellt wurde, das einen Angriff verhindert hätte. Jeder, der seine Endgeräte auf aktuellem Stand gehalten hat, war also vor dieser Attacke sicher. Es wird vermutet, dass diese Sicherheitslücke dem US-Auslandsgeheimdienst NSA bekannt war und von diesem fünf Jahre lang für eigene Zwecke eingesetzt wurde. Später kam dieses Wissen abhanden und wurde von Cyberkriminellen für die Erstellung der Schadsoftware „WannaCry“ eingesetzt (Website der Tagesschau 13.5.2017).

Neben den zahlreichen unbekannten existierenden Sicherheitslücken, gibt es etliche, weitere, die unter anderem von Geheimdiensten bewusst erzeugt oder

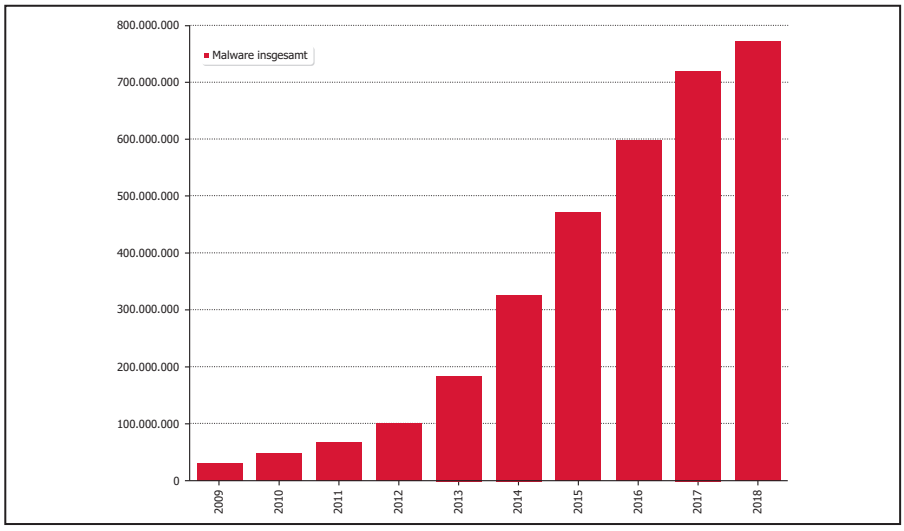


Abb. 4: Anzahl registrierter Schadprogramme pro Jahr (Quelle: AV-Test Institut)

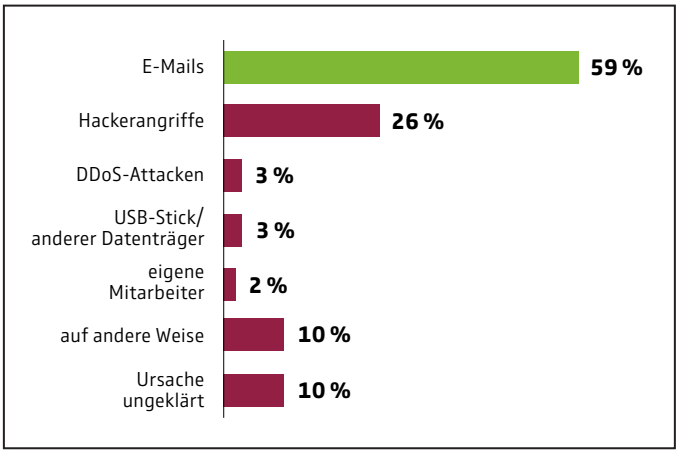


Abb. 5: Einfallstore erfolgreicher Cyberangriffe (Quelle: GDV, siehe S. 12)

geheim gehalten werden. Eine derartige Attacke kann sich jederzeit wiederholen und es kann wieder zu einem flächendeckenden Angriff auf Schwachstellen in den Systemen kommen.

Funktion und Spielarten von Cyberkriminalität

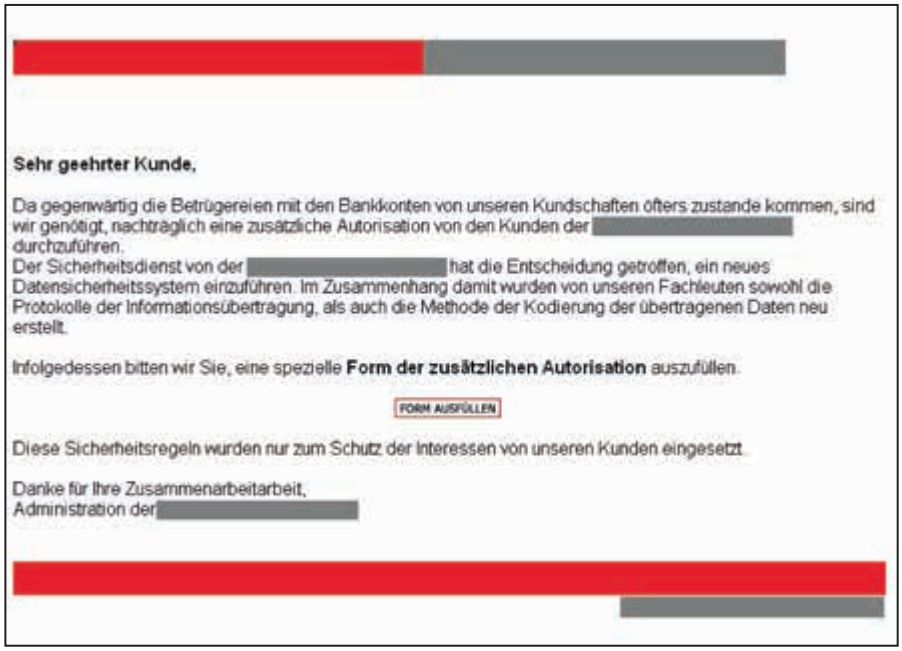
Eine der Hauptgefahren durch Cyberkriminalität stellt die Verbreitung von Schadsoftware (Malware) dar, die zu verschiedenen kriminellen Vorgängen wie Erpressung genutzt werden kann. Die Anzahl registrierter Schadprogramme stieg in den letzten Jahren massiv an (Abb. 4, Seite 3). Es gibt unterschiedliche Wege, wie eine Schadsoftware auf den eigenen Rechner gelangt. Hierbei sind grundsätzlich ungezielte Massenangriffe aus dem Internet (Schadsoftware „WannaCry“) und gezielte Angriffe auf ein System zu unterscheiden. Neben aktiven Angriffen, die in mittelständischen Betrieben vergleichsweise selten vorkommen, ist es oft der Nutzer eines Computers selbst, welcher der Schadsoftware die „Tür“ zu seinem Computer öffnet.

Hauptverbreitungswege

In der Praxis gibt es zwei **Hauptverbreitungswege** von Schadsoftware. Der mit Abstand wichtigste Verbreitungsweg ist die **E-Mail mit einem Anhang** (Abb. 5, Seite 4), in dem sich die Schadsoftware versteckt oder durch dessen Öffnung unbemerkt das Herunterladen einer Schadsoftware aus dem Internet aktiviert wird.

Es ist bekannt, dass die Bedrohungslage durch Schadsoftware mit dem allgemeinen Auftreten von Spam-E-Mails korreliert. In der Vergangenheit handelte es sich oft um E-Mails mit abstrusem Inhalt in kaum verständlichem Deutsch. Als Beispiel kennen sicherlich viele den nigerianischen Prinzen, der dem Empfänger der E-Mail aufgrund einer wirren Geschichte seine Millionen zukommen lassen will und dafür dessen Kontodaten benötigt. Heute werden solche E-Mails oft mit einem persönlichen Bezug gestaltet, um das Öffnen des Anhangs zu provozieren. Diese Technik – ein Vertrauensverhältnis vorzugaukeln – wird als Social Engineering bezeichnet. Oftmals wird der E-Mail-Empfänger mit korrektem Namen, Position und weiteren stimmigen Kontaktdetails angesprochen. Die E-Mails sind in gutem Deutsch verfasst und werden aus nachvollziehbarem Grund – beispielsweise als Bewerbungsschreiben auf eine tatsächliche Stellenausschreibung – als glaubhaft erachtet. Gegebenenfalls wird mit Firmenlogos und Signaturen gearbeitet und als Absender wird eine tatsächlich in der Firma vorkommende Person genannt. Die dabei eingesetzte E-Mail-Adresse unterscheidet sich nur in Details von derjenigen des angeblichen Absenders. Ein Teil der heute auftretenden Spam-Mails unterscheidet sich erheblich von den zuerst genannten „primitiven“ Versionen. Sie sind auch für Profis und geschultes Personal immer schwerer zu erkennen.

E-Mails werden nicht nur zur Verbreitung von Schadsoftware, sondern auch zu dem sogenannten **„Phishing“** eingesetzt. Hierbei soll der Empfänger unter Vorspiegelung falscher Tatsachen dazu ge-



Sehr geehrter Kunde,

Da gegenwärtig die Betrügereien mit den Bankkonten von unseren Kundschaften öfters zustande kommen, sind wir genötigt, nachträglich eine zusätzliche Autorisation von den Kunden der [redacted] durchzuführen.
Der Sicherheitsdienst von der [redacted] hat die Entscheidung getroffen, ein neues Datensicherheitssystem einzuführen. Im Zusammenhang damit wurden von unseren Fachleuten sowohl die Protokolle der Informationsübertragung, als auch die Methode der Kodierung der übertragenen Daten neu erstellt.

Infolgedessen bitten wir Sie, eine spezielle **Form der zusätzlichen Autorisation** auszufüllen.

FORM AUSFÜLLEN

Diese Sicherheitsregeln wurden nur zum Schutz der Interessen von unseren Kunden eingesetzt.

Danke für Ihre Zusammenarbeitarbeit,
Administration der [redacted]

Abb. 6: Beispiel für eine Phishing-Mail: In diesem Fall wurde eine bekannte deutsche Bank als Köder verwendet.

bracht werden, Zugangsdaten zu einem bestimmten Dienst (Online Banking, E-Mail, E-Shops,…) einzugeben (Abb. 6, S. 4). Es kann sich beispielsweise um eine glaubhaft wirkende E-Mail einer Bank handeln, bei der der Empfänger tatsächlich ein Konto führt. Die E-Mail fordert den Empfänger dazu auf, seine Zugangsdaten einzugeben bzw. einem Link zu folgen, der zu einem echt wirkenden „Nachbau" einer offiziellen Website (Logo etc. vorhanden) führt. Wenn man sich nun täuschen lässt und seine Daten eingibt, wird es im schlimmsten Fall für den Täter möglich, Buchungen oder Bestellungen im Namen des tatsächlichen Anwenders durchzuführen. Dies funktioniert natürlich auch mit dem Betriebskonto. Die Gefahr ist hier sogar größer, da oft mehrere Personen die Berechtigung besitzen, Buchungen durchzuführen und jeder Berechtigte getäuscht werden kann. Daher muss jedem Anwender bekannt sein, dass in der Regel kein Onlinedienst und insbesondere keine Bank den Nutzer auffordert, außerhalb des eigentlichen Anmeldevorgangs seine Zugangsdaten einzugeben.

Bei dem zweitwichtigsten Verbreitungsweg handelt es sich um **Websites mit verborgener Schadsoftware.** Oft wird dieser Weg mit einer E-Mail kombiniert, in der sich der Link zu einer solchen Website befindet. Unter Umständen genügt es, eine solche Website aufzurufen, damit das eigene System infiziert wird. Ein einziger unbedachter Klick auf einen solchen Link kann also zu einem Befall mit Schadsoftware führen.

Weitere Verbreitungswege

Eine weitere Möglichkeit der Infektion stellt das unbeabsichtigte aktive **Downloaden von Schadsoftware** dar, die sich unter anderem in kostenlos angebotenen nützlichen Programmen verbirgt. Auch auf zuverlässigen Webseiten kann sich derartige Software verbergen. Es gibt Schadsoftware, die sich über mobile Datenträger (z. B. USB-Sticks) verbreitet. Hierbei kann eine Infektion schon alleine dadurch weitergegeben werden, dass ein mobiler Datenträger von einem Endgerät an ein weiteres angeschlossen wird. Vor allem die eigenständige Verbreitung einer Schadsoftware stellt eine große Gefahr dar. Dies erklärt die schnelle und extreme Ausbreitung der Schadsoftware WannaCry. Diese suchte, sobald sie einen Computer über einen der zuvor genannten Wege infiziert hatte, selbständig nach weiteren Computern im Netzwerk, die eine für die Software brauchbare Schwachstelle enthielten und infizierte diese. Voraussetzung für die Infektion ist also eine Schwachstelle. Deshalb

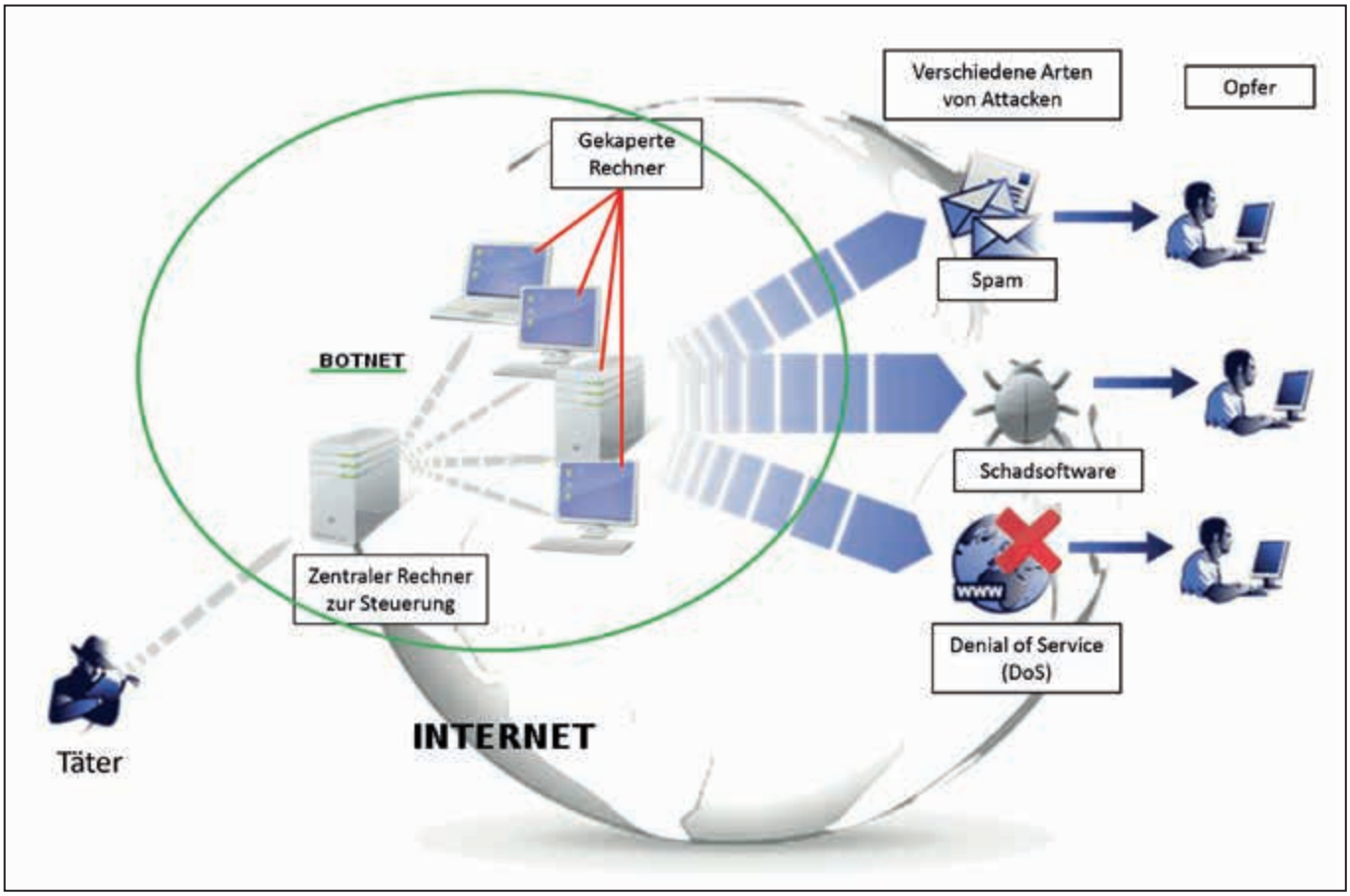


Abb. 7: Aufbau und Nutzung eines Botnetzes (Quelle: JeroenT96)

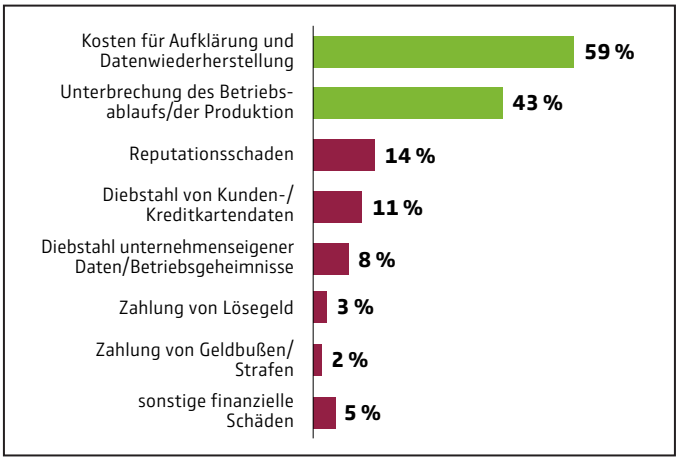


Abb. 8: Wirtschaftliche Schäden durch Cyberattacken (Quelle: GDV, siehe S. 12)

ist es wichtig, alle Systeme durch Updates auf dem aktuellen Stand zu halten. Da dieser notwendige aktuelle Stand oftmals nicht eingehalten wird, können innerhalb kürzester Zeit ganze Firmennetzwerke infiziert werden.

Hintergründe und Ziele

Ein Cyberangriff kann verschiedene Ziele haben. Neben der Erpressung durch Verschlüsselung von Daten stellt auch Spionage oder die Integration des Endgerätes in ein sogenanntes Botnetz ein lohnenswertes Motiv für Cyberkriminelle dar. Bei **Botnetzen** handelt es sich um mit Schadsoftware infizierte und untereinander vernetzte Rechner, die über einen gekaperten Server vom Täter zentral gesteuert werden können (Abb. 7, S. 5). Oft fällt diese Kaperung spät oder nie auf, da das Botnetz nur sporadisch eingesetzt wird und sich der Einsatz oft nur in einer temporären Verlangsamung des Computers auswirkt. Diese wird vom Nutzer zwar unter Umständen bemerkt, aber aufgrund fehlenden Wissens nicht als Problem eingeordnet. Heutzutage ist es sogar möglich, vorhandene Botnetze für die eigene Nutzung zu mieten. Diese Netze werden von den Cyberkriminellen für weitere Cyberattacken, Spamversand, DoS-Attacken (Webseiten werden durch sehr viele Aufrufe außer Gefecht gesetzt) und sonstige mit Cyberkriminalität im Zusammenhang stehende Tätigkeiten verwendet.

Cyberattacken betreffen heute alle mit dem Internet verbundenen Endgeräte. Neben klassischen Computern, Laptops, Tablets und Smartphones sind auch die aktuellen Smart Home-Komponenten (vernetztes Haus bzw. Wohnung) sowie Alltagsgegenstände wie PKW oder Kühlschrank, die durch das sogenannte Internet of Things (IoT) mit dem Internet verbunden sind, zu bedenken. Durch diesen heute üblichen hohen Grad der Vernetzung sind die Bürocomputer ebenso wie die Klima- oder Bewässerungssteuerungen, die über einen PC bedient werden, betroffen. Moderne Klima- und Bewässerungsanlagen sind heute aus dem Internet bedienbar. Hierdurch werden die Systeme und damit die Betriebe angreifbar. Diese Gefahr potenziert sich für alle den Cyberspace betreffenden Anwendungen drastisch, wenn unvorsichtig mit Zugangsdaten zu Systemen und Diensten umgegangen wird. Trotz bester Abwehrmechanismen sind viele Unternehmen nicht vor Risiken durch Cyberkriminalität geschützt.

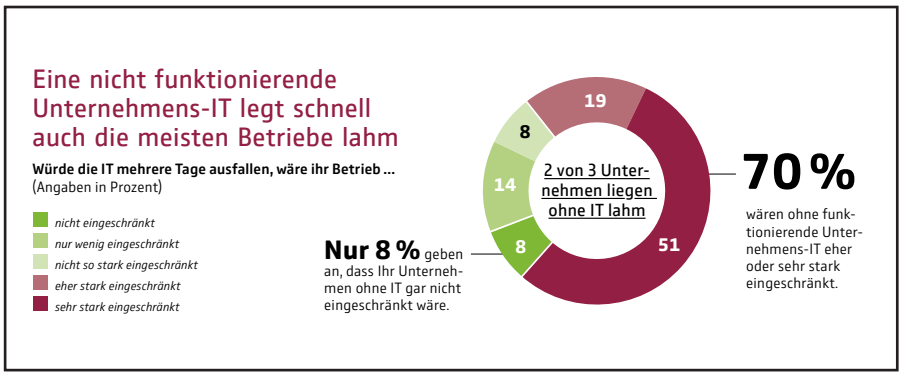


Abb. 9: Einschätzung von Unternehmen zu den Auswirkungen einer nicht funktionierenden IT auf den Betriebsablauf (Quelle: GDV, siehe S. 12)

Folgen eines erfolgreichen Cyberangriffs

In Gartenbauunternehmen stellt die Nutzung von Computern und Internet, dem Cyberspace, zur Bewältigung von betriebswirtschaftlichen, logistischen und technischen Geschäftsprozessen heute den Standard dar. Die Digitalisierung und die Vernetzung bieten allerdings eine breite Angriffsfläche für Cyberkriminelle, die insbesondere auch mittelständische Unternehmen im Fadenkreuz haben. Ein wesentlicher Grund dafür ist, dass die mittelständischen Unternehmen bei der Anwendung grundsätzlicher Sicherheitsstandards oft überfordert sind und damit ein leichtes Ziel darstellen.

Oft führt der mangelnde Cyberschutz zu verhinderbaren Schäden. Falls Ihr Betrieb Opfer von Cyberkriminalität wird, kann dies weitreichende negative Folgen für das Unternehmen bedeuten (Abb. 8, S. 6). Einzelne Rechner und ganze EDV-Netzwerke können temporär oder dauerhaft außer Gefecht gesetzt werden. Ein Ausfall der EDV-Anlage kann zu erheblichen innerbetrieblichen Störun-

gen bis zum Betriebsstillstand führen (Abb. 9, S. 6), wenn beispielsweise keine Lieferscheine mehr erstellt werden können oder Bestellungen gar nicht mehr abgerufen und damit auch nicht ausgeführt werden können. Durch einen Ausfall der Klima- oder Bewässerungssteuerung drohen Schäden an Kulturen und an Einrichtungen, Waren und Vorräten.

Häufige Folgen durch Cyberkriminalität

- Störung oder Verlust durch Hard- und Software
- Datenverlust
- Computerbetrug (z. B. Erstellung von Fake-Rechnungen im Namen Ihrer Firma)
- Erpressbarkeit durch angedrohten Datenverlust
- Betrug mit Zugangsberechtigungen
- Fälschung von Daten, Veränderungen von Daten und Parametern (z. B. bei Klima- und Bewässerungssteuerungen)
- Computersabotage (z. B. Angriff auf den Klimacomputer)
- Ausspähen von Daten (u. U. in Verbindung mit Erpressbarkeit)
- Angriff von Innen (z. B. aus Rache)

Quellen: BKA Bundeslagebild Cybercrime, HDI

Eventuell kann die Schadsoftware dazu führen, dass die vorhandene Hardware nicht weitergenutzt werden kann. In diesem Fall müssten neue Geräte angeschafft werden und mit den Betriebssystemen und den notwendigen Softwarepaketen eingerichtet werden. Auf den Geräten gespeicherte Daten, die nicht extern gesichert wurden, lassen sich häufig nicht mehr wiederherstellen! Der Schaden liegt hierbei nicht nur im direkten Verlust von Daten, Hardware oder Software, sondern vor allem in den betriebswirtschaftlichen Folgen, die aus schadenbedingten Verzögerungen im Betriebsablauf, Rufschädigung und Vertrauensverlust beim Kunden resultieren können.

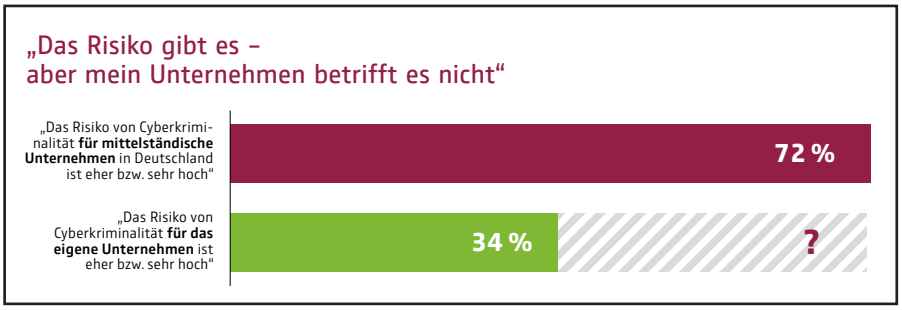


Abb. 10: Einschätzung von Unternehmen hinsichtlich des Risikos, Opfer von Cyberkriminalität zu werden – allgemein und für das eigene Unternehmen (Quelle: GDV, siehe S. 12)

Schadenverhütung – Was kann ich im Vorfeld tun?

Die vorhandenen Möglichkeiten zur Schadenprävention sind vielfältig. Dabei gibt es grundlegende Maßnahmen, die für jede Privatperson und insbesondere für jeden Betrieb den Mindeststandard an Sicherheitsvorkehrungen darstellen. Wenn kritische Bereiche über vernetzte Computer abgewickelt werden, sind erweiterte Maßnahmen zu treffen. Zuletzt stellt eine professionelle Datensicherung die einzige Möglichkeit dar, größtmögliche Sicherheit vor ungewolltem Datenverlust zu erzeugen.

➢ Basisschutz

Die wichtigste Maßnahme besteht in der Schaffung eines Risikobewusstseins bei Betriebsleitern und Mitarbeitern. Das Risiko für den eigenen Betrieb wird oft unterschätzt (Abb. 10, S. 7). Alle Mitarbeiter sollten über die Grundzüge des Cyberschutzes, vor allem das Erkennen von Spam-Mails, informiert sein. Bei der Einrichtung eines jeden im Cyberspace agierenden Computers sollten bestimmte Grundeinstellungen vorgenommen werden, um eine möglichst sichere Benutzung zu gewährleisten. Des Weiteren sollten Sicherheitsupdates von Betriebssystemen und Programmen immer sofort und im Idealfall automatisiert durchgeführt werden. Auf kritischen Rechnern sollte sich ausschließlich die notwendige Software befinden. Zu diesen Themen gibt es zahlreiche, auf die verschiedenen Betriebssysteme angepasste Anleitungen im Internet. Sehr gute Anleitungen sind auf der Webseite des Bundesamtes für Sicherheit in der Informationstechnik (https://www.bsi-fuer-buerger.de) zu finden.

Der Einsatz eines Virenscanners und einer **Firewall** ist Pflicht. Diese müssen im Idealfall automatisiert durch entsprechende Updates auf aktuellem Stand gehalten werden. Dies ist besonders wichtig, da sich neue Angriffsmöglichkeiten rasend schnell verbreiten. Es gibt kostenpflichtige Virenscanner, die eine erhöhte Sicherheit gewährleisten sollen. Zu diesem Thema sind zahlreiche Informationen und Tests in gängigen Zeitschriften und auf zahlreichen Websites vorhanden. Auch die Firewall muss immer auf dem aktuellsten Stand sein und möglichst wenige Ausnahmeregeln enthalten.

Die Nutzung **mobiler Datenträger** (CDs, USB-Sticks, externe Festplatten) und vor allem fremder Geräte, stellt ein besonderes Risiko dar. Auf diesen können sich Schadprogramme verbergen, die sich beim Anschluss des Datenträgers automatisch installieren. Es sollte festgelegt

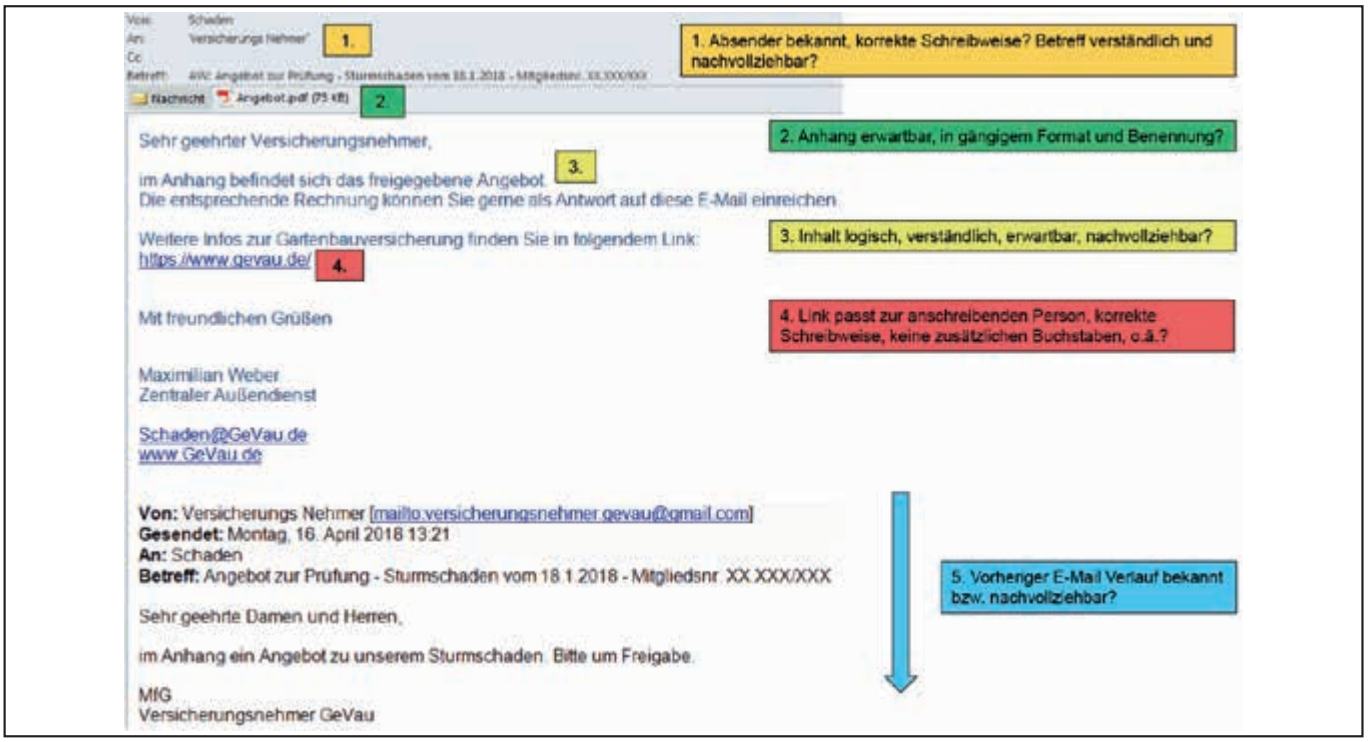


Abb. 11: Durch eine schnell durchzuführende Prüfung der aufgeführten Punkte kann die Sicherheit beim E-Mail-Verkehr enorm erhöht werden (Quelle: Gartenbau-Versicherung VVaG)

sein, wer welche Informationen von mobilen Datenträgern in das System übertragen darf. Die automatische Überprüfung auf Schadprogramme beim Einlegen oder Anschließen der Medien an einen Rechner muss aktiviert sein.

Die Erteilung der **Zugangsrechte** sollte auf die notwendigen Bedürfnisse des Nutzers beschränkt werden. Dies gilt auch für Fernzugriffe. Hierbei handelt es sich um sogenanntes „Whitelisting“. Jeder Nutzer sollte eine eigene Kennung und ein nur ihm bekanntes Passwort besitzen. Nach Möglichkeit sollten diese Daten bei Änderungen von Parametern (z. B. bei Klima- und Bewässerungssteuerungen) vom System protokolliert werden, dadurch werden Einstellungsänderungen nachvollziehbar.

Besondere Vorsicht ist bei dem Umgang mit **Passwörtern** geboten. Niemals sollten Passwörter verwendet werden, die einen persönlichen Bezug enthalten (Geburtsdatum, Adresse, …) oder die sehr einfach sind (1234). Jedes Passwort sollte einmalig sein und maximal einmal pro Dienst verwendet werden. Die Passwörter sollten von Zeit zu Zeit gewechselt werden. Insbesondere, wenn ein Datenleck bei einem Dienst bekannt wird, der vom Betrieb genutzt wird, muss das entsprechende Passwort gewechselt werden. Es gibt Programme, die bei der Erstellung und Anwendung von Passwörtern Unterstützung bieten und die durch ein Master-Passwort gesichert sind. Passwörter sollten auch nicht im Geldbeutel oder im Handy einprogrammiert mitgeführt werden. Allgemein gesagt: Wenn Probleme vermieden werden sollen, behandeln Sie Passwörter wie Ihren Bank-Pin.

Auch beim Umgang mit **E-Mails** ist Vorsicht geboten. Prüfen Sie E-Mails kritisch auf Absender und Inhalt (Abb. 11, S. 8). Dies gilt insbesondere, wenn die E-Mail Links oder Anhänge enthält. Fragen Sie sich selbst, ob ein Dienst oder gar eine Bank auf diese Weise an Sie herantreten würde. Wenn die E-Mail eine Aufforderung zur Eingabe von Zugangsdaten hat, ist dies in den seltensten Fällen mit guten Absichten verbunden. Wie im echten Leben gilt: Niemand überweist Ihnen aus nicht nachvollziehbarem Grund Geld, nur weil Sie Ihre Kontodaten angeben.

Wenn Sie **Links zu Webseiten** folgen, überprüfen Sie die URL auf Korrektheit. Auch auf gängigen Websites etablieren sich kriminelle Tätigkeiten. Als Beispiel sei hier der Betrug mit gefälschten Immobilienanzeigen genannt. Dabei werden tatsächlich existierende, aber in der Realität nicht zum Verkauf stehende Immobilien extrem günstig angeboten. Hierdurch wird versucht, mögliche Opfer zu leichtsinnigem Verhalten zu verleiten, wie beispielsweise vorab eine „Kaution“ für einen Schlüssel zu überweisen, der dann angeblich im Nachgang zugesendet wird. Diese und ähnliche Betrugsversuche laufen im Internet millionenfach ab und bleiben aufgrund der Anonymität oft ungestraft.

Bei **kostenfreien Downloads** ist höchste Vorsicht geboten. Bei vielen kostenfreien Inhalten ist unerwünschtes bis gefährliches Material enthalten.

Wenn die aufgezählten Maßnahmen nicht selbstständig durchgeführt werden können, sollte die Einrichtung der EDV- Anlage grundsätzlich durch einen Fachmann durchgeführt werden. Dasselbe gilt für große oder den Betriebsablauf relevante Anlagen. Spätestens ab diesem Punkt sollten erweiterte Schutzmaßnahmen getroffen werden.

➢ **Erweiterter Schutz**

Es empfiehlt sich Systeme voneinander zu trennen. Der Rechner, auf dem das Klima- oder Bewässerungsprogramm läuft, sollte als eigenständiger Rechner laufen. Bei der Aufstellung einer kompletten EDV-Anlage sollte darauf geachtet werden, dass die Umgebungsbedingungen (wie Temperatur, Luftfeuchtigkeit, Staub) den vorgegebenen Anforderungen der Anlage entsprechen. Die Anlagen sollten gegen Elementarschäden (Feuer, Wasser, Blitz und Überspannung) geschützt werden.

Ebenso sollte der Aufstellort Schutz vor Diebstahl und unberechtigtem physischen Zugriff bieten. Dauerhaft genutzte Netzwerkanschlüsse müssen vor unberechtigter Nutzung geschützt werden. Dies kann unter anderem durch physische Zugriffs- oder Zutrittsbeschränkungen, einer Deaktivierung der Netzwerkanschlüsse oder durch eine Authentifizierung des Nutzers geschehen.

Ferner sollte mit der betreuenden Firma über Möglichkeiten der Wiederherstellung gesprochen werden. Auch sollte geprüft werden, wie schnell im Schadenfall die entsprechende Hard- und Software zur Verfügung gestellt und eingerichtet werden kann. Spezielle Softwarepakete sollten an mindestens zwei verschiedenen Orten mit den aktuellen Einrichtungen zur Verfügung stehen. Als zusätzlichen Schutz bieten IT-Firmen Dienstleistungen, wie die Überwachung der EDV, Installation der anstehenden Updates für Betriebssysteme, Antivirenprogramme sowie Programme zur Aktualisierung der Firewall an.

➢ **Datensicherung und Archivierung**

Die absolute Grundlage des Cyberschutzes ist es, durch eine Datensicherung die Integrität und Verfügbarkeit von wichtigen Daten sicherzustellen. Datensicherung ist der einzige (fast) hundertprozentig sichere Weg, den Folgen eines Cyberangriffes vorzubeugen. Durch eine dem Betrieb sinnvoll angepasste Datensicherung ist es möglich, verlorene Daten in kurzer Zeit wiederherzustellen und so den Betrieb aufrechtzuerhalten.

Die Sicherung der Daten kann auf folgenden Wegen stattfinden:

1. Sicherung relevanter Daten auf **externen Medien** (Festplatte, USB usw.):

Es ist darauf zu achten, dass es mehrere Generationen von Sicherungsmedien gibt, die in regelmäßigen Intervallen (z. B. wöchentlich) gewechselt werden. Angeschlossene Medien können bei einer Attacke mit befallen werden. Die Lagerung der gespeicherten Daten sollte zudem in einem anderen Gebäude(-teil) stattfinden, um auch bei einem Brand in der Anlage eine verwendbare Sicherung zu besitzen. Der Nachteil: Manuelle Eingriffe sind nötig, die gewissenhaft ausgeführt werden müssen.

2. Sicherung in einem **NAS-Speicher** (Netzwerk-Speicherplatz):

Bei einem NAS-Speicher handelt es sich um ein eigenständiges Gerät, das ausschließlich für das Backup von Daten eingesetzt wird (ohne Nutzung weiterer möglicher Funktionen). Dieses Gerät funktioniert eigenständig ohne angeschlossenen steuernden PC. Ein Vorteil von NAS-Systemen ist der Standort z.B. in einem anderen Brandabschnitt oder in einer anderen Filiale (abhängig von der Datenmenge und der zur Verfügung stehenden Bandbreite). Die Datensicherung wird mit einem Backup-Programm, welches zum NAS-System dazugehört, automatisch durchgeführt. Dieses kann mehrere Generationen von Sicherungssätzen auf einer NAS ablegen. Der Zugriff auf die NAS, erfolgt nur, während das Backup durch die Software ausgeführt wird. Ansonsten sollte die NAS für das Computersystem nicht erreichbar sein. Somit ist die Gefahr, dass dieses System befallen wird, eher gering. Der Vorteil dieses Szenarios ist der Automatismus. Über den Erfolg der Datensicherung wird via E-Mail informiert, somit ist der Vorgang dokumentiert. Rücksicherungen der Daten sind als Test in regelmäßen Abständen durchzuführen, um die erfolgreiche Sicherung zu verifizieren.

3. Sicherung in einer **Cloud** (online auf einem externen Server im Internet):

Bei einer Cloud werden die Daten auf dem Server eines Unternehmens abgelegt, das den benötigten Speicherplatz – vergleichbar zur Miete – anbietet. Die Prozesse der Speicherung laufen wie bei einem NAS-Speicher automatisiert ab. Es besteht die Möglichkeit, mehrere Sicherungsintervalle abzuspeichern. Zur sicheren Nutzung wird jedoch auch hier eine Datensicherungssoftware benötigt. Daten sollten verschlüsselt abgelegt und der Schlüssel mehrfach an verschiedenen Standorten gespeichert werden, da bei Verlust kein Zugriff mehr möglich ist. Cloud-Lösungen weisen eine physikalische Trennung zum ursprünglichen Speicherort auf, so dass auch bei einer Totalzerstörung der Hardware, beispielsweise in einem Brandfall, noch auf die Daten zugegriffen werden kann.

Der komfortablen Nutzung einer Cloud stehen als Nachteile die laufenden Kosten und die Abhängigkeit zum Anbieter sowie das Thema Sicherheit gegenüber. Es besteht grundsätzlich die Möglichkeit unerwünschter Fremdzugriffe beispielsweise im Rahmen eines „gewöhnlichen" Cyberangriffs auf den Cloud-Anbieter. Des Weiteren gibt es keine Sicherheit, dass Firmen ausschließlich dem deutschen Gesetz unterliegen, so dass je nach Unternehmens-/Serverstandort oder Art der verwendeten Software Zugriffe ausländischer Behörden (beispielsweise aus den USA) durchaus möglich sind. Diese Behörden haben dann deutlich ausgeweitete Befugnisse, um sich einen umfassenden Datenzugriff zu ermöglichen. Man gibt in diesem Fall seine Daten und damit die wichtigsten Informationen des Unternehmens in die Hände Dritter. Ein Cloud-Dienst zur Datensicherung von Unternehmen stellt daher keine optimale Lösung dar.

- **Empfehlungen zum Vorgehen im Schadenfall**

Oft versuchen Unternehmen Cybervorfälle eigenständig aufzuarbeiten, selbst wenn sie nicht über ausreichend Kapazitäten und Fachwissen verfügen. Das führt zur Vergrößerung von Schäden, da die Aufklärung des Vorfalls verzögert wird. Unklare Zuständigkeiten, Fehler in Beweissicherung und Kommunikation haben oft irreparable Auswirkungen. Ist ein Angriff erkannt worden, besteht zügiger Handlungsbedarf. In der Praxis sollten nun Fachfirmen herangezogen werden. Idealerweise handelt es sich um die IT-Firma, die den Betrieb ohnehin betreut und mit dem Umfang und den Anwendungen des vorhandenen IT-Systems vertraut ist. Im Vordergrund steht jetzt die Wiederherstellung der Systeme und eventuell verlorengegangener Daten.

Zunächst muss der Zeitpunkt des Angriffs eingegrenzt werden. Auf diese Weise ist eine Datenwiederherstellung zum letzten „gesunden" Zustand eines Systems möglich. Es sollte möglich sein, die Daten im sogenannten *Read-Only-Modus* zu analysieren, um prüfen zu können, ob weiterhin ein Befall mit Schadprogrammen vorliegt. Dies gilt unabhängig von der eingesetzten Methode der Datensicherung. Vor der Reaktivierung der Systeme sollten die Abwehrmechanismen nochmals überprüft werden, um einen neuerlichen erfolgreichen Angriff auszuschließen. Bei einem länger andauernden Totalausfall lohnt es sich, wenn die Betriebsabwicklung auch unabhängig von vernetzter Technik aufrechterhalten werden kann. Dazu können beispielsweise Lieferscheine in Papierform bevorratet und per Hand ausgefüllt werden. Ein Notfallplan, der die Zuständigkeiten im Falle eines länger andauernden Ausfalls der IT regelt (z. B. ein Gießplan), hilft dabei, unnötige Folgeschäden zu vermeiden.

Fazit

So hilfreich die zahlreichen Möglichkeiten sind, die sich durch die weitreichende Vernetzung von Hardware ergeben, so anfällig ist das System für Manipulationen und Cyberkriminalität. Die Gefahr für einen ungezielten Angriff ist vor allem für mittelständische Unternehmen hoch, da diese oft keine ausreichende Manpower und Fachwissen im Unternehmen vorhalten können, um sich mit dieser zusätzlichen Problematik zu beschäftigen. Für viele Gartenbauunternehmen liegen die Prioritäten in anderen Bereichen, nämlich dem Produzieren, Veredeln und Verkaufen hochwertiger pflanzlicher Produkte – und damit ihrem eigentlichen Geschäft. Trotz der Gefahren, die sich durch Cyberkriminalität ergeben, ist es für die meisten Unternehmen sicherlich nicht zielführend, auf die Nutzung vernetzter Technik zu verzichten. Die Anwendung digitaler Prozesse wird sich auch im Gartenbau weiterhin enorm vergrößern. Wenn dies nicht bereits geschehen ist, wird die Nutzung vernetzter Hardware einen Grundpfeiler aller Unternehmen darstellen. Die Unternehmen der Gartenbaubranche sollte sich frühzeitig mit diesen Themen beschäftigen.

Einiges, was in diesem Beitrag zur Betriebssicherheit aufgeführt wurde, unter anderem die Schaffung eines Gefahrenbewusstseins oder die automatisierte Durchführung von Updates, kann sofort und eigenständig durchgeführt werden. Für viele weitere Maßnahmen ist die Beauftragung von Fachfirmen notwendig. Hierdurch lässt sich ein abgesicherter digitaler Betriebsablauf gewährleisten. Im Idealfall geschieht dies, bevor ein Schadenereignis eingetreten ist. Viele durch Cyberkriminalität verursachte Schäden sind durch verhältnismäßig einfache und günstige Sicherheitsmaßnahmen zu vermeiden. Das vorhandene Risiko ist von keinem Betriebsleiter zu unterschätzen. Jeder erfolgreich abgewehrte Cyberangriff spart Kosten und Zeit.

Abschließend bleibt festzustellen, dass keine absolute Cybersicherheit erreicht werden kann. Es ist aber möglich, die Sicherheit durch das Einhalten einiger Grundsätze enorm zu erhöhen. Beachten Sie dazu bitte die Checkliste auf Seite 11.

Ausblick

Auch die Gartenbau-Versicherung ist bei diesem Thema sensibilisiert und arbeitet aktuell daran, weiterreichenden Versicherungsschutz, gegebenenfalls gemeinsam mit spezialisierten Firmen, für die Bedürfnisse des Gartenbaus zu fairen Konditionen bereitzustellen. Aktuell können Kulturen im Rahmen einer Verderbschadenversicherung gegen unbefugte Einwirkung auf Steuerungs- und Kontrolleinrichtungen versichert werden, solange diese Anlagen nach dem Stand der Technik gesichert sind.

Checkliste

Überprüfen Sie regelmäßig den aktuellen Cyberschutz im Betrieb

- Sind Antiviren- bzw. Firewall-Programme installiert und auf dem aktuellen Stand?
- Sind die Betriebssysteme auf die neuesten Versionen aktualisiert?
- Ist eine ausreichende Datensicherung vorhanden, werden die Speichermedien regelmäßig überprüft bzw. ausgetauscht? Funktioniert die vorhandene Datensicherung auch ordnungsgemäß?
- Wird eine manuelle Datensicherung regelmäßig ausgeführt und überprüft?
- Werden Mitarbeiter/innen regelmäßig zum Thema IT-Sicherheit sensibilisiert?
- Gibt es einen Hauptverantwortlichen für die IT-Sicherheit im Betrieb?
- Besteht für Notfälle (insbesondere Cybervorfälle) ein Notfallkonzept und wird dieses regelmäßig getestet?

Erste Maßnahmen nach einem Cyberangriff

Grundsätzlich ist hier Eile geboten, um den Schaden möglichst gering zu halten! Sofern Sie kein Fachmann sind, holen Sie sich schnell Hilfe von einem externen IT-Spezialisten!

- Trennen Sie das betroffene Gerät vom Netzwerk bzw. vom Internet, um eine interne oder auch externe Verbreitung zu vermeiden.
- Prüfen Sie den Umfang des Schadens und grenzen Sie ihn ein.
- Stellen Sie fest, seit wann die Schädigung erfolgt ist.
- Gehen Sie nicht auf Lösegeldforderungen ein.
- Nutzen Sie Antiviren- bzw. Malware-Scanprogramme, um die Ursache zu finden.
- Löschen Sie betroffene Dateien von Ihrem System bzw. nutzen Sie die Funktionen von entsprechenden Programmen zur Virendefinition und -entfernung.
- Stellen Sie Ihre Dateien aus einem Backup wieder her, das vor dem Befallszeitpunkt erstellt wurde und prüfen Sie, ob alle Funktionen wieder zur Verfügung stehen und ob das Gerät wieder von allen „Schädlingen“ befreit ist.

Gartenbau-Versicherung VVaG
Von-Frerichs-Straße 8
65191 Wiesbaden

Tel. 0611 / 56 94 - 0
Fax 0611 / 56 94 -140

service@GeVau.de
www.GeVau.de

Ein Unternehmen in der AgroRisk Gruppe

Autoren:
B. Sc. Maximilian Weber,
Herbert Janssen

Fotos:
Titelbild: Inkje von Wurmb,
Erstveröffentlichung im Magazin
„Gemüse“, Nr. 2/2018
Seite 9: *GV*

Grafiken:
GDV, Forsa-Befragung 2018
„Cyberrisiken im Mittelstand“

© Gartenbau-Versicherung 09/2018