38

CYBERSCHUTZ IM GARTENBAU

Ihr 3-Punkte-Plan:

- Risikobewusstsein
- IT-Infrastruktur
- Cyberversicherung

Mit separater Check-liste!

GARTENBAU VERSICHERUNG

INHALT

Als separates Formular anbei (und als Download verfügbar):

Checkliste IT-Sicherheit.

1. CYBERSCHUTZ: Schaffen Sie digitale Sicherheit für Ihren Betrieb.

Dass der Gartenbau Opfer von Cyberkriminalität sein kann, zeigt ein Fall aus der Praxis: In einem Topfpflanzenbetrieb waren Produktion und Handel, die gesamte Hardware, Computer, Server und selbst die Drucker von einem Cyberangriff betroffen. Die E-Mail-Adressen der Mitarbeitenden mussten gelöscht und neu angelegt werden. Telefonanlage und Warenwirtschaftssystem fielen aus, selbst die Warenannahme und -auslieferung war zeitweise unmöglich. Der Betrieb konnte erst nach Wochen wieder richtig anlaufen.

Dieser Angriff ist kein Einzelfall. „Es besteht dringender Handlungsbedarf, sich als Unternehmen vor Cyberangriffen zu schützen“, betont Luca Schetter, Cyberexperte der Gartenbau-Versicherung. Denn digitale Prozesse sind aus dem modernen Betriebsalltag nicht mehr wegzudenken – denken Sie etwa an Mailverkehr, Rechnungswesen, Steuerung des Klimacomputers, der Bewässerungssysteme und PV-Anlagen.

Dementsprechend steigen die Anforderungen an die IT-Sicherheit. Cyberangriffe können jeden treffen – unabhängig von Betriebsgröße oder Branche.

Ein einziger Klick auf einen infizierten E-Mail-Anhang kann ausreichen, um zentrale Systeme lahmzulegen. Die Folgen: Produktionsausfälle, Datenverlust und erhebliche wirtschaftliche Schäden.

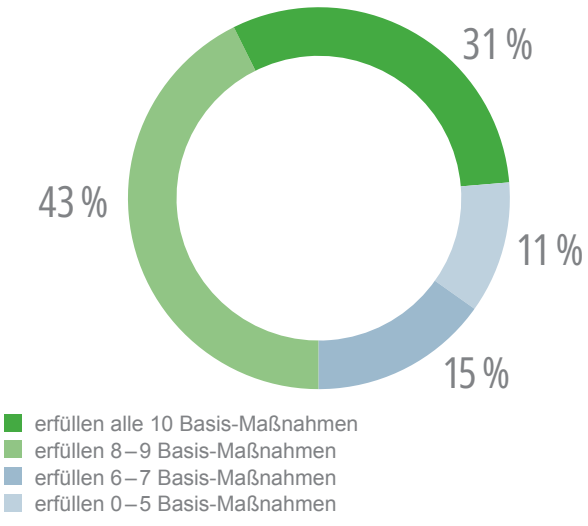
Umso wichtiger ist es, frühzeitig vorzusorgen. Wir unterstützen Sie dabei, Ihre digitale Infrastruktur zu schützen – mit praxisnahen Empfehlungen, verlässlichen Partnern und dem Hinweis auf sinnvolle Absicherungen wie eine Cyberversicherung. Denn wer vorbereitet ist, bleibt handlungsfähig – auch im Ernstfall.

2. CYBERRISIKEN im Mittelstand – gemeinsam vorbeugen.

Die Forsa-Umfrage „**Cyberrisiken im Mittelstand 2024**“, durchgeführt im Auftrag des Gesamtverbands der Versicherer (GDV), zeigt, dass kleine und mittlere Unternehmen ein sehr hohes Risiko haben, Opfer von Cyberangriffen zu werden. Die Gründe: Sie überschätzen oft die eigene IT-Sicherheit und unterschätzen die Gefahr eines Cyberangriffs auf das eigene Unternehmen.

IT-Sicherheit mittelständischer Unternehmen zeigt deutliche Lücken

Nur eine Minderheit erfüllt den Basisschutz vollständig

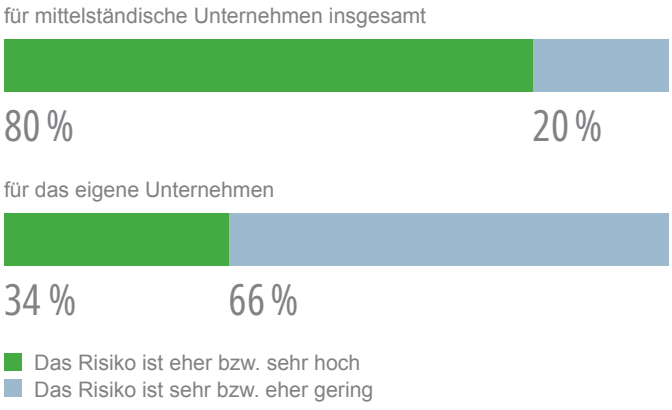


Quelle: *GDV Gesamtverband der Versicherer, Repräsentative Forsa-Befragung 300 mittelständischer Unternehmen 2024*

Auch das Bundeslagebild Cybercrime 2024 des Bundeskriminalamtes offenbart: Die Bedrohungslage durch Cyberkriminalität ist anhaltend hoch. Und kleine und mittelständische Unternehmen sind oftmals Ziel der Angriffe: Sie machen laut BKA rund 80 % der von Ransomware*-Angriffen betroffenen Unternehmen aus.

Das Risiko gibt es – aber mein Unternehmen betrifft das nicht

Frage: Wie schätzen Sie das Risiko ein, Opfer von Cyberkriminalität zu werden?



Quelle: *GDV Gesamtverband der Versicherer, Repräsentative Forsa-Befragung 300 mittelständischer Unternehmen 2024*

** Ransomware beschreibt Schadsoftware, die Dateien auf einem Computer verschlüsselt oder den Zugriff auf das Gerät sperrt, um dann ein Lösegeld für die Freigabe zu fordern (vgl. Seite 6).*

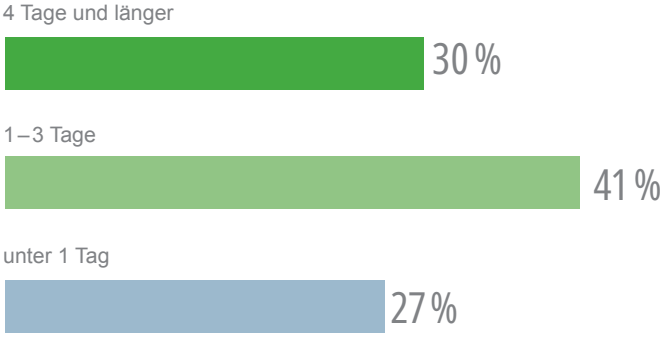
Cyberangriffe können jeden treffen, der mit dem Internet verbundene Server, Computer, Tablets, Smartphones oder sonstige Endgeräte nutzt. Kein moderner Gartenbaubetrieb kommt heute ohne diese Technik und ihre digitalen Funktionen aus. Ein Ausfall der IT-Infrastruktur führt in der Regel zu beachtlichen Folgekosten, zusätzlicher Arbeit und enormem Stress. Es ist nicht zu unterschätzen, wie lange es dauert, bis die Systeme wieder laufen. Daher ist Cyberschutz so wichtig.

Digitale Sicherheit beginnt mit einem realistischen Blick auf Ihre IT-Infrastruktur. Wenn Sie wissen, wo mögliche Schwachstellen liegen, können Sie gezielt handeln.

Genau dabei unterstützen wir Sie: mit verständlicher Beratung, praxisnahen Lösungen und einem klaren Fokus auf Prävention.

Cyberattacken legen Unternehmen oft tagelang lahm

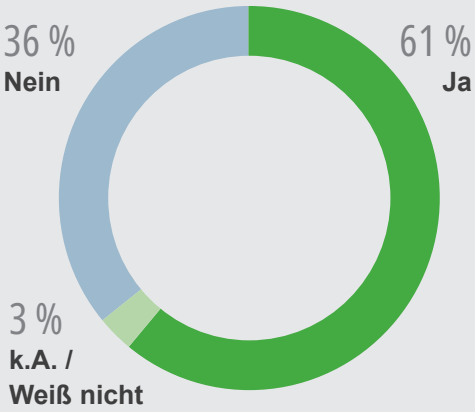
Wie lange hat es gedauert, die IT-Systeme wiederherzustellen und die Schadsoftware zu beseitigen?



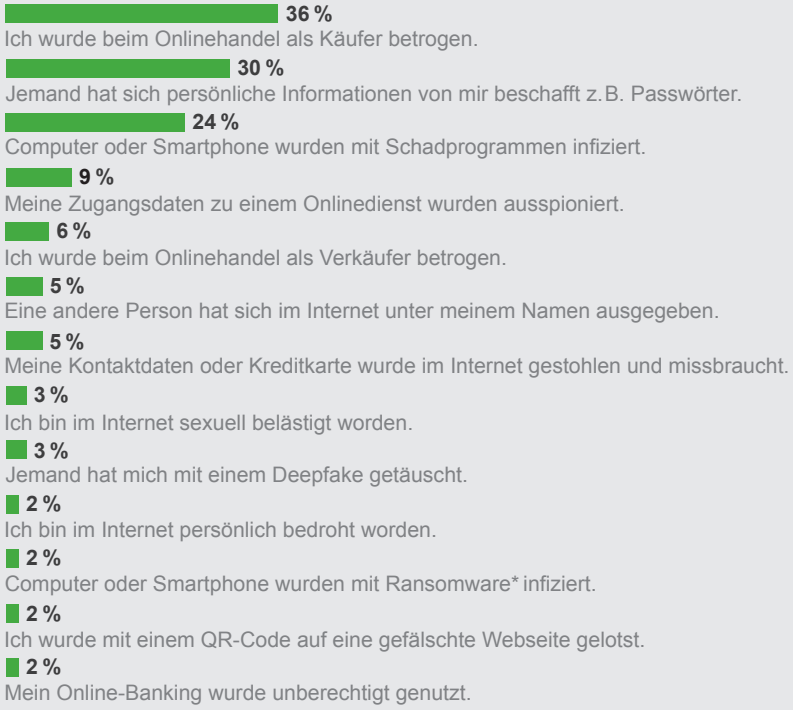
Quelle: *GDV Gesamtverband der Versicherer, Repräsentative Forsa-Befragung 300 mittelständischer Unternehmen 2024*

Kriminalität ist im Internet weit verbreitet

Haben Sie in den vergangenen 12 Monaten Erfahrungen mit Cyberkriminalität im Internet gemacht?



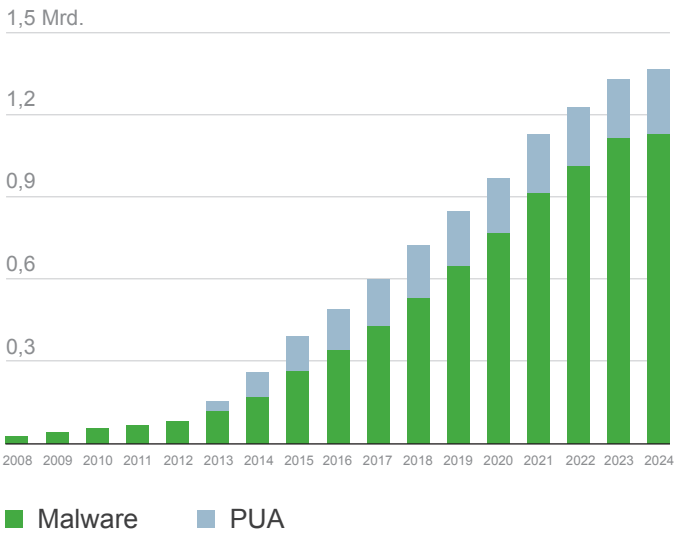
Basis: *Internetnutzerinnen und -nutzer (n=1.021), Mehrfachnennungen möglich (rechts)*
Quelle: *Bitkom Research 2025*



3. CYBERGEFAHREN im Überblick.

Schadsoftware (Malware)

Schadsoftware, auch Malware genannt, nennt man Programme, die unbemerkt auf internetfähige Geräte wie Computer, Smartphone, Tablet, Router, Netzwerkspeicher oder IoT-Geräte* geladen werden. Grundsätzlich können alle Geräte, die mit dem Internet verbunden sind und Software verwenden, davon befallen sein. Die Anzahl registrierter Schadprogramme ist in den letzten Jahren massiv gestiegen – ein klarer Hinweis darauf, wie dynamisch und ernst die Bedrohungslage ist (vgl. Abbildung).



Das AV-Test Institut registriert täglich mehr als 450.000 neue Schadprogramme und potentiell unerwünschte Anwendungen (PUA).

Quelle: *av-atlas.org*

Die Ziele, die Cyberkriminelle mit Malware verfolgen, sind vielfältig: Erpressung, Datendiebstahl (Passwörter, Bankdaten, Unternehmensdaten, u. s. w.) Geräteübernahme und vieles mehr.

Verbreitungswege von Malware

- E-Mails mit infizierten Anhängen oder Links
- Fake-Webseiten oder infizierte Werbung
- infizierte USB-Sticks oder Software-Downloads
- Sicherheitslücken in veralteter Software

Erpressung mit Ransomware

Eine spezielle Form von Malware ist Ransomware. Einmal unbemerkt installiert, verschlüsselt sie Dateien oder ganze Systeme, oft auch die Sicherheitskopien (Backups), wenn diese nicht sicher aufbewahrt werden. Das Ziel ist eindeutig: Die Täter fordern Lösegeld (engl. ransom) von den Opfern, damit die Entschlüsselung aufgehoben wird.

Malware läuft oft unbemerkt im Hintergrund: um Daten abzugreifen, zu spionieren oder Dinge zu kontrollieren. Ransomware hingegen meldet sich aktiv bei den Opfern, um sie zu erpressen.

Tipp
Ein wirksamer Schutz gegen Ransomware beginnt mit regelmäßigen, offline gesicherten Backups und einer geschulten Aufmerksamkeit im Umgang mit E-Mail-Anhängen und Links. Wenn Sie technische Sicherheitsmaßnahmen mit klaren Verhaltensregeln kombinieren, reduzieren Sie das Risiko deutlich.

** IoT-Geräte sind physische Objekte mit integrierten Sensoren und Software, die Daten sammeln, senden und empfangen, um über das Internet miteinander und mit Systemen zu kommunizieren. In einem Gewächshaus können IoT-Bodenfeuchtesensoren genutzt werden, die kontinuierlich den Wassergehalt der Erde messen und diese Daten an ein zentrales Bewässerungssystem senden. Dieses passt automatisch die Wasserzufuhr an die Bedürfnisse der Pflanzenkulturen an und sendet Alarme, wenn kritische Werte erreicht werden.*

Gerätemissbrauch im Botnetz

Botnetze sind mit Schadsoftware infizierte, untereinander vernetzte Endgeräte, die vom Täter ferngesteuert werden können. Oft fällt das erst spät oder nie auf, da das Botnetz nur sporadisch genutzt wird und man außer einer kurzfristigen Verlangsamung des Computers nichts bemerkt.

Über Botnetze werden Webseiten lahmgelegt, Spam-E-Mails versendet oder auch Passwörter geknackt. Cyberkriminelle können sich heutzutage auf einschlägigen Plattformen sogar Botnetze mieten, um damit ihre Cyberangriffe durchzuführen.

Tatsächlich ist es möglich, dass ein eigenes Gerät unwissentlich Teil eines Botnetzes ist. Dann ist nicht nur das Gerät selbst in Gefahr, sondern es wird auch zur Gefahr für andere.

Tipp

Achten Sie darauf, Ihr Betriebssystem und alle Programme stets aktuell zu halten – Sicherheitsupdates schließen bekannte Schwachstellen, bevor sie ausgenutzt werden können. Installieren Sie außerdem eine zuverlässige Antivirensoftware und überprüfen Sie regelmäßig Ihr Gerät auf verdächtige Aktivitäten. So schützen Sie nicht nur sich selbst, sondern auch andere vor dem Missbrauch Ihres Geräts.

Phishing

Phishing werden Täuschungsversuche genannt, die darauf abzielen, dass die Empfänger freiwillig vertrauliche Daten preisgeben ohne zu merken, dass sie einem Betrug aufgesessen sind. Phishing wird im Prinzip über alle (digitalen) Kanäle gestreut und wirkt oft täuschend echt. Dabei setzen die Cyberkriminellen zunehmend auch auf KI-Tools, was den Betrug immer schwerer erkennbar macht. Letztendlich erzeugen die Täter mit Phishing Druck, Angst oder Vertrauen, um ihre Opfer dazu zu bringen, Daten, Geld oder beides herauszugeben – und dabei im guten Glauben zu sein, das Richtige zu tun. Das trifft nicht nur Privatleute, sondern auch Unternehmen. Wenn Zugangsdaten zu Ihrem Betriebskonto herausgegeben werden, kann das schmerzhafte Folgen haben.

Verbreitungswege von Phishing-Attacken

- gefälschte E-Mails mit gefährlichen Anhängen und/oder manipulierten Links
- falsche Infos per SMS oder Messenger-Dienst (WhatsApp, Signal, Telegram u. a.)
- betrügerische Telefonanrufe
- betrügerische Kontakte/Links über Social Media

Phishing-Versuche sind heute schwer erkennbar. Früher waren es oft abstruse Mails, die relativ leicht als Betrug erkennbar waren, wie die von einem vermeintlichen nigerianischen Prinzen, der dem Mail-Empfänger hohe Summen überweisen möchte und daher dessen Bankdaten benötigt. Solche plumpen Versuche sind selten geworden. Heute gehen die Täter subtiler vor. Sie nutzen öffentlich zugängliche Informationen (aus Social Media, Firmenwebsite u. a.), um Informationen über die Opfer zu sammeln und sich dann als jemand auszugeben, der vertrauenswürdig ist.

Tipp

Seien Sie wachsam bei E-Mails, die Sie zur Eingabe persönlicher Daten oder zum Klick auf unbekannte Links auffordern – selbst wenn sie scheinbar von vertrauenswürdigen Absendern stammen. Überprüfen Sie die Absenderadresse genau und geben Sie sensible Informationen niemals über unsichere Webseiten preis. Ein gesundes Maß an Skepsis schützt Sie vor Täuschungsversuchen.

Und was ist mit Spam?

Spam ist im Vergleich zu Phishing relativ „harmlos“. Denn hier haben die Absender vor allem ein Ziel: verkaufen. Sie haben oft reißerische Betreffzeilen und wollen dazu animieren, Werbung anzuklicken. Das kostet Zeit und Nerven, ist aber meist nur lästig, nicht gefährlich.

Tipp

Installieren Sie einen zuverlässigen Spamfilter und ignorieren Sie verdächtige Nachrichten konsequent. So bleibt Ihr Posteingang sauber und Sie schützen sich vor unnötiger Ablenkung.

Warum Menschen Betrügern aufsitzen: Social Engineering

Social Engineering setzt auf psychologisches Feingefühl. Statt die Technik zu hacken, hacken die Täter das Verhalten der Menschen. Sie stellen gezielt Fragen, erschleichen sich Vertrauen oder üben Druck aus – bis Sie selbst die digitale Tür öffnen: durch das Anklicken eines Links, das Installieren eines Programms oder das Preisgeben sensibler Daten.

Oftmals wird der E-Mail-Empfänger mit korrektem Namen, richtiger Position und weiteren stimmigen Kontaktdetails angesprochen. Die E-Mails sind in gutem Deutsch verfasst und werden aus nachvollziehbarem Grund – beispielsweise als Bewerbungsschreiben auf eine Stellenausschreibung – als glaubhaft erachtet. Auch Firmenlogos, Signaturen und Absender sind meist nur schwer als Fälschung erkennbar.

Tipp

Bleiben Sie wachsam, besonders bei unerwarteten Anfragen – auch wenn sie vertrauenswürdig wirken. Geben Sie niemals persönliche Informationen preis, ohne die Echtheit des Absenders eindeutig zu prüfen.

Schwachstellen in der eigenen IT-Struktur

Schwachstellen in der IT-Struktur erleichtern es Kriminellen zusätzlich, ihre Angriffe durchzuführen. Fehlende Sicherheitsupdates, Standardpasswörter, ungeschützte Geräte wie WLAN-Router, Kameras oder Maschinensteuerungen sowie fehlende oder ungetestete Backups sind typische Einfallstore. Wer sich ausschließlich auf sein Kerngeschäft konzentriert und die IT-Sicherheit vernachlässigt, riskiert mehr als nur einen Systemausfall – im schlimmsten Fall steht der gesamte Betrieb still.

Tipp
Machen Sie IT-Sicherheit zur Chefsache. Regelmäßige Wartung, klare Zuständigkeiten und ein durchdachtes Sicherheitskonzept schützen nicht nur Ihre Technik, sondern auch Ihre Pflanzen und Geschäftsprozesse.

Häufige Folgen der Cyberkriminalität

- Störung oder Verlust von 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*

4. CYBERSCHUTZ: So sorgen Sie vor!

1 RISIKOBEWUSSTSEIN SCHAFFEN

Es ist extrem wichtig, dass Betriebsleitung und Mitarbeitende über Cybergefahren Bescheid wissen. Sie müssen das Risiko kennen und die Gefahren realistisch einschätzen. Und sie müssen wissen, wie man sich richtig verhält. Denn die Mitarbeitenden sind oft unbewusst das Einfallstor für Cyberangriffe. Daher raten wir Ihnen, Schulungen zu Cybersicherheit durchzuführen und Merkblätter bereit zu halten.

Hier nennen wir Ihnen die wichtigsten Basics, die Ihr ganzes Team kennen sollte:

E-Mails und Links kritisch prüfen

Absender, Inhalt und Links sollten immer kritisch geprüft werden. Die Aufforderung, Zugangsdaten einzugeben, ist meist sehr verdächtig.

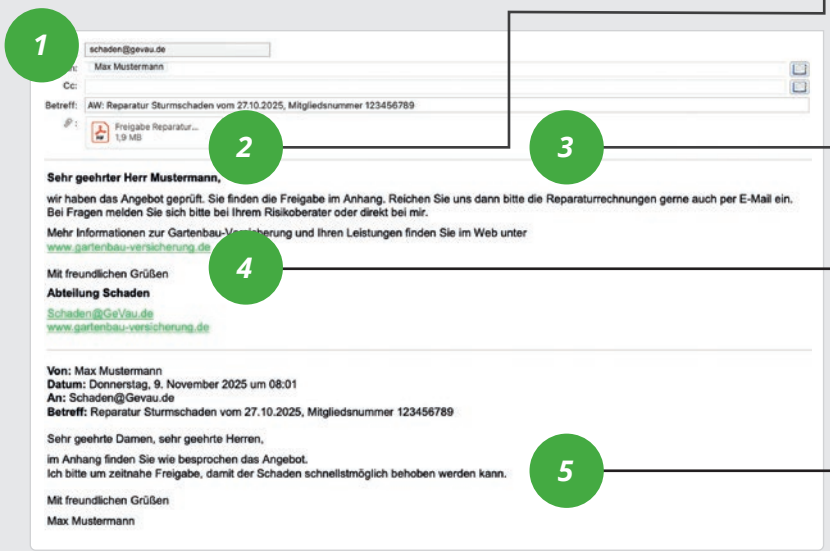
Überprüfen Sie mittels Mouse-Over-Effekt zuerst die Absenderadresse und die bei Links hinterlegte URL. Denken Sie daran: Auch auf bekannten Internetseiten gibt es Betrug. Ein Beispiel: Hochwertige Maschinen oder seltene Pflanzen werden auf Internet-Portalen extrem günstig angeboten. Die Betrüger verlangen eine Vorauszahlung, etwa für Versand oder als Anzahlung. Danach hört man nichts mehr von ihnen. Solche Betrugsmaschen bleiben meist unbestraft, weil die Täter nicht ausfindig gemacht werden können.

Nutzung mobiler Datenträger und fremder Geräte

Auf USB-Sticks, externen Festplatten oder anderen mobilen Datenträgern könnte sich Schadsoftware verbergen und automatisch installieren, sobald die Datenträger oder Geräte angeschlossen werden. Daher sollten Sie genau festlegen, wer welche Informationen

Checkliste zum sicheren Umgang mit E-Mails

Punkt 1:
- Absender bekannt, korrekte Schreibweise?
- Betreff verständlich und nachvollziehbar?



Punkt 2:
- Anhang erwartbar?
- Anhang in gängigem Format und Benennung?

Punkt 3:
- Inhalt logisch und verständlich?
- Inhalt erwartbar und nachvollziehbar?

Punkt 4:
- Link passt zur anschreibenden Person?
- Korrekte Schreibweise?
- keine zusätzlichen Buchstaben o.ä.?

Punkt 5:
- Vorheriger Mailverlauf bekannt bzw. Mailverlauf nachvollziehbar?

von externen Quellen ins System übertragen darf. Wichtig ist zudem eine automatische Überprüfung auf Schadsoftware.

Zugangsrechte beachten

Jeder Beschäftigte arbeitet mit einem eigenen Benutzerkonto und erhält ausschließlich Zugriff auf die Systeme, die für seine Aufgaben wichtig sind – nach dem Prinzip der minimalen Rechte. Dann wird für Sie nachvollziehbar, wer welche Änderungen bei der Klima- und Bewässerungssteuerung vorgenommen hat. Nur wenige in Ihrem Team sollten Administrator-Rechte haben. Ein dauerhafter Login als Administrator ist zu vermeiden. Auch müssen die Zugangsrechte mindestens jährlich geprüft und nötigenfalls aktualisiert werden – zum Beispiel, wenn Mitarbeitende ausscheiden oder intern neue Aufgaben übernehmen.

Passwörter sicher erstellen und aufbewahren

Verwenden Sie keine Passwörter mit persönlichem Bezug, Namen oder einfache Kombinationen wie „admin123“. Und nutzen Sie niemals ein Passwort für mehrere Konten. Denn wird es gehackt, sind gleich mehrere Konten betroffen. Um sich Passwörter zu merken, können Sie einen Passwort-Manager nutzen. Ganz wichtig: Hinterlassen Sie keine Notizen mit den Passwörtern am Schreibtisch oder im Portemonnaie.

Vorsicht bei kostenlosen Downloads

Kostenlose Downloads wirken oft harmlos, können aber versteckte Schadsoftware enthalten. Besonders gefährlich sind Angebote, die auf unbekannten oder unseriösen Webseiten stehen, in verdächtigen E-Mails verlinkt sind oder beim Download zusätzliche Programme oder Browser-Erweiterungen mit installieren.

Tipp

Laden Sie Software nur von offiziellen und bekannten Quellen herunter. Installieren Sie niemals Software, die Zugriffsrechte aufs ganze System verlangt und lassen Sie Downloads vor dem Öffnen über ein Antivirenprogramm prüfen.

IT-Verantwortlichkeiten klären & Abläufe planen

Ein fester Ansprechpartner für IT-Fragen sorgt dafür, dass sich jemand zuständig fühlt und weiß, was bei Updates, Sicherheitsfragen und einem Cyberangriff zu tun ist. Genauso wichtig ist ein Notfallplan. Dieser sollte folgende Fragen beantworten: Wer muss informiert werden? Welche Systeme sind besonders kritisch? Wo liegen die Backups? Wer entscheidet über Abschalten oder Wiederherstellen?

2 IT-INFRASTRUKTUR OPTIMIEREN

Die Grundeinstellung der Rechner

Die Grundeinstellungen Ihrer Rechner sind der Basisschutz, der eingerichtet werden sollte, bevor Ihr PC mit dem Internet oder Netzwerk verbunden wird. Dazu zählen unter anderem:

- **Virenscanner & Firewall**
  Virenscanner und Firewall sind Pflicht. Sie müssen mit regelmäßigen Updates auf aktuellem Stand gehalten werden, damit sie den stets neuen Angriffsmöglichkeiten gewachsen sind. Es gibt kostenpflichtige Virenscanner, die eine erhöhte Sicherheit gewährleisten sollen. Informieren Sie sich über aktuelle Tests in IT-Zeitschriften und auf entsprechenden Ratgeber-Websites.
- **Sicher eingestellte E-Mail-Programme**
  Hier müssen Phishing- und Spam-Filter aktiv sein, die Vorschau von Anhängen deaktiviert werden und es darf kein automatisches Laden externer Inhalte erlaubt sein.
- **Automatische System- und Software-Updates**
  Aktivieren Sie automatische Updates für Betriebssysteme sowie für Software-Programme (auch Browser, PDF-Reader, Office) und deinstallieren Sie unnötige Programme. Das mindert die Angriffsfläche für Cyberkriminelle. Gute Anleitungen für verschiedene Betriebssysteme finden Sie auf der Website des Bundesamtes für Sicherheit in der Informationstechnik (https://www.bsi-fuer-buerger.de – einfach bei der Suche „automatische Updates einrichten“ eingeben).

Das sichere Aufstellen der EDV-Anlagen

Es ist sinnvoll, verschiedene Systeme voneinander zu trennen. Steuerungsrechner für Klima- oder Bewässerungssysteme sollten eigenständig betrieben werden, nicht gemeinsam mit Büro- oder Internetanwendungen. So bleiben kritische Funktionen auch bei Angriffen oder Störungen geschützt.

Achten Sie darauf, dass Umgebungsbedingungen wie Temperatur, Luftfeuchtigkeit und Staubbelastung den Herstellervorgaben entsprechen. Und denken Sie daran, die Anlagen vor Feuer, Wasser, Blitzschlag und Überspannung zu schützen, z. B. durch Überspannungsschutz, Rauchmelder oder erhöhte Aufstellung. Nicht zuletzt sollte der Aufstellort vor unbefugtem Zugriff geschützt sein – durch abschließbare Räume, Schränke oder Zugangskontrollen. Genauso wenig dürfen die Netzwerkanschlüsse offen zugänglich sein. Möglich sind physische Zugangsbeschränkungen, deaktivierte Netzwerkanschlüsse bei Nichtnutzung und die Absicherung des Zugangs mittels Authentifizierung.

Datensicherung & Archivierung

Die zuverlässige Datensicherung schützt Ihr Unternehmen im Ernstfall. Wer regelmäßig sichert, kann wichtige Daten schnell wiederherstellen und den Betrieb aufrechterhalten. Die drei gängigsten Sicherungsmethoden sind:

a) Auf externen Speichermedien
Behalten Sie nicht nur eine einzige Sicherungskopie, sondern mehrere, die auf unterschiedlichen Datenträgern und zu unterschiedlichen Zeitpunkten erstellt wurden. Die Datenträger bitte nicht angeschlossen lassen, denn sie könnten sonst bei einem Angriff mitverschlüsselt werden. Am besten bewahren Sie diese außerhalb des Betriebsgebäudes an einem sicheren Ort auf.

b) Auf NAS-Speicher (Netzwerk-Speicherplatz)
Ein NAS-Speicher ist ein eigenständiges Gerät für Backups. Er wird ans Netzwerk angeschlossen, aber nicht an den PC – und kann daher auch an einem anderen Standort stehen. Die Datensicherung wird mit einem Backup-Programm automatisch durchgeführt. Es können hier auch mehrere Generationen von Sicherungen abgelegt werden. Der Zugriff auf den NAS erfolgt nur während des Backups, ansonsten ist er für den Computer nicht erreichbar. Das senkt die Gefahr eines Cyberangriffs. Der Vorteil: Einmal eingerichtet, läuft alles automatisch und Sie werden per Mail über die Datensicherung informiert. Dennoch gilt: Rücksicherungen der Daten sind als Test in regelmäßen Abständen durchzuführen, um die erfolgreiche Sicherung zu verifizieren.

c) In der Cloud
Bei der Cloud-Sicherung werden Daten automatisiert auf den Servern eines externen Anbieters gespeichert – vergleichbar mit gemietetem Speicherplatz. Die Sicherung erfolgt wie beim NAS, aber online. Sie brauchen also auch eine Datensicherungssoftware. Wichtig ist, dass die Daten verschlüsselt gespeichert werden und der Schlüssel sicher aufbewahrt wird, da sonst kein Zugriff möglich ist. Ein Vorteil: Die Daten sind räumlich vom Betrieb getrennt und damit auch bei Brand oder Diebstahl geschützt.

Tipp
Niemand kann Experte für alles sein. Wenn Sie die hier genannten Cyberschutz-Maßnahmen nicht selbständig durchführen können, ziehen Sie einen IT-Experten hinzu.

Fragen Sie auch nach KI-Tools, die Sie zum Cyberschutz einsetzen können. Denn die KI kann als „digitaler Sicherheitsassistent“ eingesetzt werden und bei ungewöhnlichen Aktivitäten wie nächtliche Logins Alarm schlagen. Hier unbedingt erfahrene Fachleute hinzuziehen.

Cybersicherheit für PV- und Agri-PV-Anlagen

Die Wechselrichter und Speicherbatterien in PV- und Agri-PV-Anlagen sind über die Leistungselektronik und die Steuerung in der Regel mit dem Netz gekoppelt – und daher auch potenziell durch Cyberkriminalität gefährdet.

Besprechen Sie die Risiken mit Ihrem Partner für Solartechnik oder den Risikoberatern der Gartenbau-Versicherung. In der Regel sorgen die Hersteller der Systeme durch regelmäßige Updates für möglichst lückenlose Sicherheit. Dennoch ist es wichtig, dass Sie hierfür ein klares Risikobewusstsein entwickeln, Ihre Systeme auf Schwachstellen prüfen und auch einen Notfallplan entwickeln.

3 CYBERVERSICHERUNG ABSCHLIESSEN

Trotz effizienter Cyberschutz-Maßnahmen kann Ihr Betrieb Opfer eines Cyberangriffs werden. 100-prozentige Sicherheit gibt es leider nicht. Zumal die Cyberkriminellen immer neue Wege entwickeln, die Systeme zu hacken.

Um sich gegen die Folgen erfolgreicher Cyberangriffe zu schützen, empfiehlt sich daher der Abschluss einer Cyberversicherung. Die Gartenbau-Versicherung bietet Ihnen hier modulare Lösungen, die sich genau an Ihren Bedarf anpassen lassen.

Das Basispaket enthält Versicherungsschutz gegen Schäden

- durch Beschädigung, Zerstörung, Veränderung, Blockierung oder Missbrauch der eigenen Betriebssysteme
- an Programmen und Daten infolge eines Hackereinbruchs
- durch Cybererpressung

Es lässt sich erweitern um speziellen Versicherungsschutz gegen

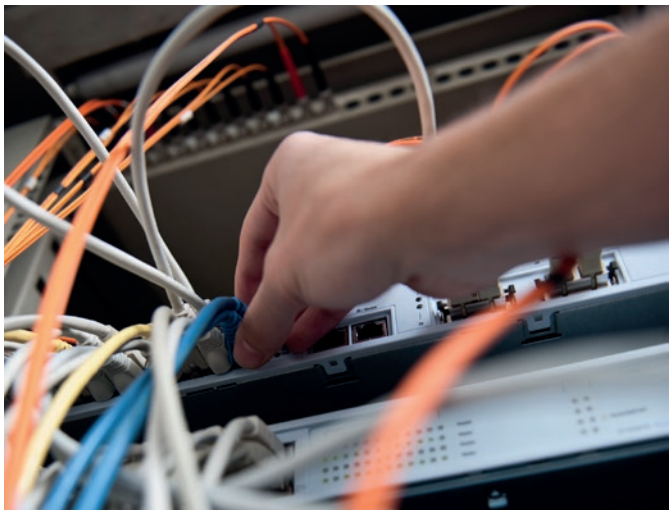
- Zahlungsmittelschaden
- Betriebsunterbrechung
- Vertrauensschaden
- Haftpflichtschaden, im Zusammenhang mit einem Cyberangriff

Unsere maßgeschneiderte Absicherung bietet Sicherheit und schnelle Wiederherstellung im Falle eines Angriffs aus dem Netz. Sie ist dank variabler Laufzeiten sehr flexibel und im Ernstfall können Sie sich auf die schnelle und unbürokratische Schadenregulierung verlassen. Darüber hinaus erhalten Sie Zugang zu einer Cyber-Hotline mit 24-Stunden-IT-Support und IT-Forensik.

Am besten lassen Sie sich einmal ausführlich dazu beraten. Sprechen Sie einfach Ihren Risikoberater darauf an und besuchen Sie unsere Website:

www.gartenbau-versicherung.de/sicherheit/cyberschutz

5. Was tun bei einem *CYBERANGRIFF?*



Grundsätzlich ist Eile geboten, um den Schaden gering zu halten. Ziehen Sie am besten einen externen IT-Spezialisten hinzu, falls Sie nicht selbst Experte in diesem Bereich sind.

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

Checkliste IT-Sicherheit – So schützen Sie sich vor Cyberkriminalität!

Überprüfen Sie anhand unserer Checkliste, ob Sie alles getan haben, um sich erfolgreich vor Cyberangriffen zu schützen.
Die Checkliste liegt der Broschüre als praktisches Einzelformular bei.

Alternativ können Sie es über folgenden Link im Internet abrufen:
www.gartenbau-versicherung.de/wp-content/uploads/checkliste-cyber.pdf

Ihr persönlicher Risikoberater oder Ihre Risikoberaterin im Außendienst berät Sie gerne – sprechen Sie uns einfach an!

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

Telefon: +49 611 5694-0
Telefax: +49 611 5694-140
E-Mail: service@gevau.de
www.gartenbau-versicherung.de
Ein Unternehmen in der AGRORISK Gruppe

Autor: Luca Schetter
Luca Schetter studierte Gartenbau und stieg 2018 bei der Gartenbau-Versicherung ein. Von der Schadenabteilung über die Sachbearbeitung bis hin zum Risikomanagement kennt er die verschiedenen Arbeitsbereiche sehr gut. Aktuell im Vertriebsmanagement angesiedelt, ist er Länderbeauftragter Polen und betreut federführend das Thema Cyberschutz.

Redaktion: Ulla Ruths
Bilder: Gartenbau-Versicherung, Adobe-Stock

CHECKLISTE
IT-Sicherheit.

GARTENBAU VERSICHERUNG

So schützen Sie sich vor Cyberkriminalität!

1. Geräte & Software

- ☐ PCs, Laptops und Tablets regelmäßig aktualisieren
- ☐ Betriebssysteme, Steuerungssoftware und Apps auf dem neuesten Stand halten
- ☐ Antivirenprogramm auf allen Geräten installiert
- ☐ WLAN & Router mit sicherem Passwort geschützt (kein Standardpasswort)

2. E-Mail & Kommunikation

- ☐ Anhänge und Links in E-Mails nur öffnen, wenn Absender bekannt und plausibel
- ☐ Verdächtige E-Mails sofort löschen – nie auf Links klicken!
- ☐ Mitarbeitende über Cybergefahren informieren (Schulung und Merkblatt)
- ☐ Regelmäßige Kontrolle: Gibt es Mails, die merkwürdig oder gefälscht wirken?

3. Zugangsdaten

- ☐ Für jedes System (E-Mail, Buchhaltung, Webshop etc.) ein eigenes starkes Passwort vergeben
- ☐ Keine Passwort-Notizen am Monitor oder unter der Tastatur
- ☐ Zwei-Faktor-Authentifizierung (2FA) aktiviert, wo möglich (z.B. Onlinebanking)

Tipp

Einmal im Quartal alle Punkte kurz durchgehen – kleine Schritte helfen, große Schäden zu verhindern.

4. Datensicherung (Backup)

- ☐ Regelmäßiges Backup aller wichtigen Daten (z.B. Kundenliste, Dokumente, Steuerungssysteme)
- ☐ Backup auf externem Medium (nicht ständig mit dem Internet verbunden)
- ☐ Wiederherstellung des Backups schon getestet?

5. Organisation & Vorbereitung

- ☐ Ansprechpartner für IT-Fragen im Betrieb bestimmt
- ☐ Notfallplan: Was tun bei Virenbefall oder verdächtiger E-Mail?
- ☐ Alle Mitarbeitenden informiert: Im Zweifel lieber nachfragen, nicht klicken

6. Internetfähige Geräte im Betrieb (IoT)

- ☐ Geräte wie Sensoren, Klimasteuerung oder Heizungsanlagen geschützt
- ☐ Standardpasswörter geändert
- ☐ Nur vertrauenswürdige Hersteller im Einsatz
- ☐ Fernzugriff nur mit Passwort + Schutz aktivieren

Cyber-Versicherungsschutz

- ☐ Versicherungsschutz prüfen
- ☐ ggf. Beratung durch Gartenbau-Versicherung

Checkliste auch als Download verfügbar:
www.gartenbau-versicherung.de/wp-content/uploads/checkliste-cyber.pdf

www.gartenbau-versicherung.de