

IT-Sicherheit ist kein Projekt, sondern eine Daueraufgabe für Unternehmen jeder Größe. Die FEGIME Deutschland lud ein IT-Unternehmen ein, um Elektrogroßhändlern Wege zu mehr Cybersicherheit zu zeigen. Ein bewährtes Konzept der IT-Spezialisten: Schutz und Service in die Cloud zu legen. Das klingt interessant genug, um diese Idee zu teilen



Sicherheit in der

Ein Virus treibt den anderen an. Die Verunsicherung durch den Corona-Virus haben die kriminellen Hacker dazu genutzt, um mit ihren Viren viel Schaden anzurichten. Das zeigt der aktuelle Bericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI), der wie alle Jahre im Oktober erschien.

Aber auch unabhängig von der Pandemie wächst gleichzeitig mit der Digitalisierung die Hacker-Szene, die sich zu einer arbeitsteilig funktionierenden »Industrie« entwickelt hat. Ob private PCs, Wasserwerke, Behörden, Krankenhäuser oder Unternehmen: Alle werden angegriffen. Erpressungssoftware (ransom ware) wird dabei immer mehr eingesetzt.

Alarmstufe rot

Im Februar 2021 notierte das BSI den höchsten jemals gemessenen Wert an neuen Schadprogramm-Varianten: Täglich kamen durchschnittlich 553.000 neue Varianten hinzu. Insgesamt wurden im Berichtszeitraum 144 Millionen neue Schadprogramm-Varianten gezählt, 22 Prozent mehr gegenüber dem Vorjahreszeitraum.

Die E-Mail ist das häufigste Einfallstor für Cyberangriffe. Schutz bieten technische Maßnahmen – und die regelmäßige Schulung der Mitarbeiter.



»Im Bereich der Informationssicherheit haben wir – zumindest in Teilbereichen – Alarmstufe Rot«, sagte BSI-Präsident Arne Schönbohm. »Der neue Lagebericht des BSI zeigt deutlich wie nie: Informationssicherheit ist die Voraussetzung für eine erfolgreiche und nachhaltige Digitalisierung.«

Den IT-Schutz vorantreiben

Auch die Großhändler der FEGIME Deutschland haben diese Entwicklung im Blick. Nun, die europaweit größte Datenbank für elektrotechnische Produkte mit über sechs Millionen Artikeln wird geschützt wie Fort Knox. »Außerdem arbeiten wir in diesem Bereich nur mit Eigenentwicklungen unseres Tochterunternehmens Geneon«, sagt Arnold Rauf, Geschäftsführer der FEGIME Deutschland.

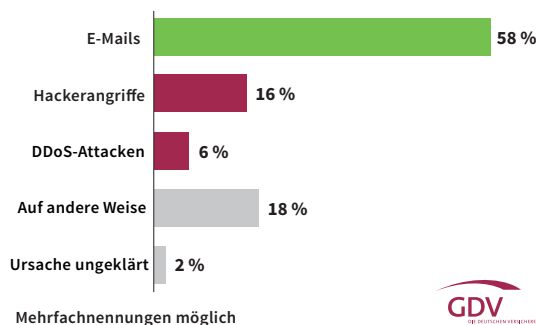
Das leicht angreifbare Standard-Backend gibt es deshalb nicht.

»Aber dennoch ist es wichtig, wie sich auch jeder einzelne unserer Großhändler bestmöglich schützt«, sagt Rauf. Deshalb lud er vor kurzem Rolf Börner ein, Geschäftsführer des IT-Spezialisten NetPlans. »Wir fanden NetPlans interessant, weil das Unternehmen Lösungen für kleinere und mittlere Unternehmen anbietet. Wir wollten sehen, welche Wege praktikabel sind und zu mehr IT-Sicherheit führen.«

Börner begann seine Präsentation mit einer Schilderung der aktuellen Risiken. Aber die Lösungen standen im Vordergrund. Jeder kennt die üblichen einfachen Maßnahmen: sichere Passwörter, regelmäßige Sicherheitsupdates, ein Daten-Backup, das den Namen auch verdient sowie der vorsichtige Umgang mit E-Mails. »Diese Maßnahmen können privat ausreichen, bei Unternehmen genügt das heute nicht«, sagt Börner.

Gefährliche Post

Erfolgreiche Cyberangriffe erfolgten durch ...



CYBER
SICHER

GDV
GEMEINSCHAFT DER
ELEKTROGROßHÄNDLER

Quelle: Repräsentative Forsa-Befragung von 300 Entscheidern in kleinen und mittleren Unternehmen im April 2020. © www.gdv.de

Handfester Schutz in der Cloud

Nun kann man Spezialisten wie NetPlans damit beauftragen, sich nur um die IT-Sicherheit zu kümmern. Dann kommen hoch entwickelte Firewall-, Passive Malware- und weitere Sicherheits-Lösungen zum Zug.

Ein anderer Weg führt in die Cloud. Wir alle nutzen Cloud-Lösungen im Alltag: Unsere Mails liegen auf den Servern des Pro-

Einfach eine Frage des Vertrags: Diese Tabelle zeigt, welche Teile seiner IT man in die Cloud von NetPlans auslagern kann. Darüber hinaus zeigt die Tabelle, um welche Aspekte der Technik man sich kümmern muss, wenn es um IT-Sicherheit geht.

Bilder: iStockphotos

Cloud

Im Unternehmen	Infrastruktur als Service	Plattform als Service	Software als Service
Applikationen	Applikationen	Applikationen	Applikationen
Daten	Daten	Daten	Daten
Runtime	Runtime	Runtime	Runtime
Betriebssystem	Betriebssystem	Betriebssystem	Betriebssystem
Virtualisierung	Virtualisierung	Virtualisierung	Virtualisierung
Backup	Backup	Backup	Backup
Server	Server	Server	Server
Storage	Storage	Storage	Storage
Netzwerk	Netzwerk	Netzwerk	Netzwerk

Betriebsverantwortung im Unternehmen
 Betriebsverantwortung bei NetPlans

viders, größere Daten-Mengen versenden wir gerne über die Drop-Box und Updates für Virens Scanner kommen auch vom fremden Server. Und immer mehr Software ist nur noch als Abonnement, über die Cloud, verfügbar.

Diese Entwicklung hat NetPlans systematisiert und zu einem Service entwickelt, der sich in vielen Unternehmen seit Jahren bewährt. »Wir bieten an, Teile der IT oder sogar die ganze in unsere Cloud-Lösungen zu übertragen«, erklärt Börner (Grafik oben). Praktisch heißt das: Die Daten liegen dann sicher und DSGVO-konform im Hochsicherheits-Rechenzentrum in Karlsruhe. Profis sorgen dort rund um die Uhr für die Sicherheit und Hochverfügbarkeit.

Den Erfolg der Digitalisierung sichern

Um den Vorteil dieses Weges zu verdeutlichen, benutzt Börner das Bild von der Autobahn: »Wir sorgen dafür, dass unsere Kunden mit ihren Daten und Anwendungen immer sicher und störungsfrei unterwegs sein können.«

Ist das auch fürs Handwerk relevant? Die nahe Zukunft gibt die Antwort: Der Stundenzettel wird abgelöst durch digitale Erfassung der Daten via Tablet oder Smartphone, die Website muss so sicher sein wie der Mailserver – und verlorene Daten einer KNX-Konfiguration oder BIM-Planung werden die Kunden und Partner gewiss nicht schätzen.

Je digitaler die Betriebsprozesse werden, desto wichtiger wird die Cybersicherheit – das gilt für kleine wie große Unternehmen. Auch NetPlans betreibt für die eigene Sicherung einen hohen Aufwand. »Einmal im Jahr laden wir Hacker ein«, sagt Börner. »Bei einem so

genannten Penetrations-Test (im IT-Deutsch »Pen-Test«) dürfen sie dann versuchen, in unsere Systeme einzudringen.«

IT-Sicherheit ist kein Projekt, sondern eine Daueraufgabe. Ebenso wird klar, dass die Absicherung der Digitalisierung Zeit und Geld kostet. Aber was kostet die IT-Sicherheit in der Business-Cloud von NetPlans? Bezüglich der Kosten verspricht Börner, dass sie »mittelfreundlich« seien und sehr transparent. Zum Faktor Zeit sagt er: »Unsere Kunden können sich auf ihr Geschäft konzentrieren, gewinnen dadurch Freiräume und können in Sachen Cybersicherheit sicher besser schlafen.«

Drei Schritte zu mehr Sicherheit

Besonders in kleineren Unternehmen sind Chef oder Chefin in der Regel auch für die IT-Sicherheit zuständig. Börner hat Verständnis für alle, die das selbst in die Hand nehmen: »Das kostet zwar extrem viel Zeit, ist aber zum Ausgleich eine sehr spannende Aufgabe.«

Der Umzug in die Cloud ist dagegen ein überschaubares Projekt. Der erste Schritt besteht aus der ersten Analyse der IT und ob eine Cloud-Lösung sinnvoll und wirtschaftlich umsetzbar ist. Es folgt ein erstes Angebot.

Im zweiten Schritt wird ganz präzise untersucht, wie die Infrastruktur und Prozesse aussehen und ob und wo der Einsatz der Cloud sinnvoll ist. Dabei werden alle wirtschaftlichen, technischen, rechtlichen sowie organisatorischen Konsequenzen berücksichtigt. Es folgt der Plan für die Umsetzung und ein Angebot mit den kalkulierbaren monatlichen Kosten.

Der dritte und letzte Schritt ist die Implementierung. Dazu gehören auch die Tests mit Feintuning und Fehlerbehebung, die durch Techniker vor Ort durchgeführt werden. Am Ende folgen die Inbetriebnahme der Cloud-Dienste, ein Review mit Dokumentation und die Abnahme.

Zu dieser technischen Seite der Cybersicherheit komme die menschliche, sagt Börner. »Zu einem umfassenden Sicherheitskonzept gehört auch die regelmäßige Schulung der Mitarbeiter. Auch das bieten wir an.«

Info, Versicherung und mehr

- Wer **umfassende Info** über das Thema sucht, findet sie beim Bundesamt für Sicherheit in der Informationstechnik (BSI). Das BSI gibt auch Unterstützung beim Einrichten des IT-Grundschutzes. Dabei handelt es sich aber nicht um eine Art Basisabsicherung – schon dieser IT-Grundschutz ist so komplex, dass er für Kleinstunternehmen kaum umsetzbar ist, also Unternehmen bis 9 Beschäftigte und bis 2 Millionen Euro Jahresumsatz.

www.bsi.de

- Wer sich für die **Cloud-Lösungen** von NetPlans interessiert, findet Info unter

www.netplans.de

- Wer sich aktiv um seine IT-Sicherheit kümmert, kann eine **Versicherung** gegen Schäden durch Cyberangriffe abschließen.

➔ **mehr in diesem Heft ab Seite 32**