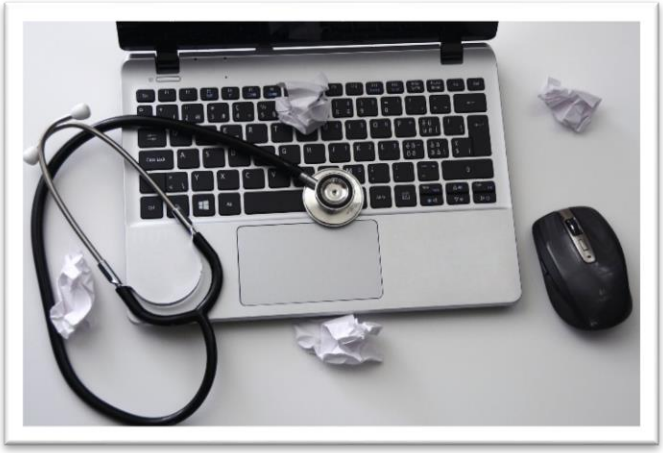
IT Spezialisten auf Abruf: Warum besonders kleinere Unternehmen von externen IT Dienstleistern profitieren

Schwandorf, 11. Juni 2019 – Egal ob ein einziger PC oder hunderte - die IT ist in fast allen Unternehmen unabdingbar und benötigt dementsprechend technisches Know-how. Bei kleineren Betrieben trägt sich eigenes IT Personal meist nicht, deshalb erledigen oftmals Mitarbeiter IT Aufgaben neben ihrer eigentlichen Arbeit. Das bindet nicht nur unnötig Personalressourcen, es birgt auch einige Gefahren und kann letztlich unterm Strich zu hohen Kosten und existenzgefährdenden Sicherheitsbedrohungen führen. Mit einer professionellen Betreuung der IT sparen kleinere Unternehmen in mehrerlei Hinsicht.

Bestellungen, Rechnungen, Buchhaltung, Korrespondenz… fast alle Bereiche eines Unternehmens werden inzwischen digital erledigt. Und die dazu benötigten Geräte sowie die eingesetzte Software sind störungsanfällig, teilweise auch erklärungsbedürftig. Dabei spielt die Anzahl der Mitarbeiter bzw. des IT Equipments keine Rolle.

Im Gegensatz zu größeren Unternehmen, rechnet sich der Einsatz einer eigenen IT Abteilung in kleineren Unternehmen fast immer rein wirtschaftlich nicht.



„Herumdoktern" an IT Systemen kann mehr Schaden als Hilfe anrichten. Bild: annca/Pixabay

Die Geschäftsleitung kleinerer Unternehmen ist oftmals der Meinung, dass sie für ihre wenigen PCs keine externe Hilfe in Anspruch nehmen muss und betrauen Mitarbeiter damit, anfallende technische Probleme, neben ihrer regulären Arbeit zu lösen. Selbst wenn diese Mitarbeiter durch ihren privaten PC eine prinzipielle Ahnung haben, so fehlt ihnen meist das technische Know-how, um alle Probleme sinnvoll lösen zu können. Dies führt oft zu „Flickschusterei", die sich am Ende nicht auszahlt und besonders in Hinblick auf IT Sicherheit schlimmstenfalls zu massiven, existenzgefährdenden Problemen führen kann.

1. Die Folgen fehlender IT Kompetenz

1.1 Schäden durch Cyber-Angriffe

Existentielle Bedrohungen für Unternehmen jeder Größe

Unternehmen jeder Größe und Branche sehen sich heutzutage ständig den Gefahren aus dem Internet ausgesetzt. Nachfolgend eine kleine Auswahl der „gängigsten" Bedrohungen:

- Schadprogramme (Malicious Software, kurz: Malware) und alle Unterarten wie Ransomware (sperrt den Zugang zu den Computerdaten und fordert „Lösegeld), Computerwürmer, Trojaner, Spyware, etc.
- Hacking: Illegaler Zugriff auf computer- bzw. personenbezogene Systeme
- DDoS-Angriffe (Distributed Denial of Service): Zielsysteme und Internetservices werden durch Überlastung für den Benutzer nicht mehr oder nur stark eingeschränkt nutzbar
- CEO Fraud-Attacken: Im Namen des Firmenchefs oder einer vergleichbaren Instanz wird, mithilfe gefälschter, aber täuschend echt wirkender eMails, beispielsweise die Buchhaltung aufgefordert, eine Zahlung auf ein (meist ausländisches) Konto vorzunehmen.

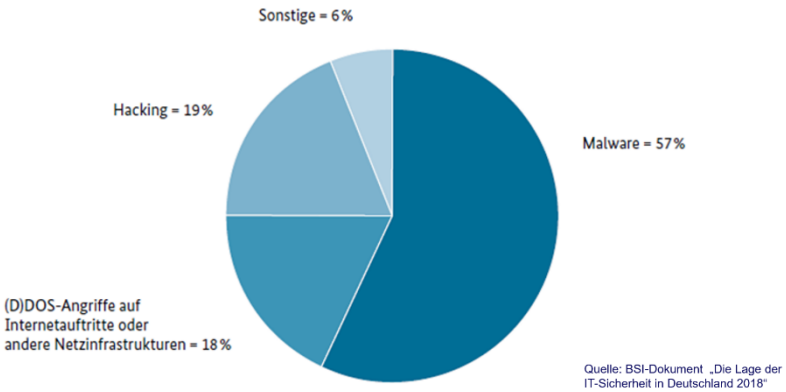
Pressekontakt:

Inez Paulus
Abteilungsleiterin Marketing

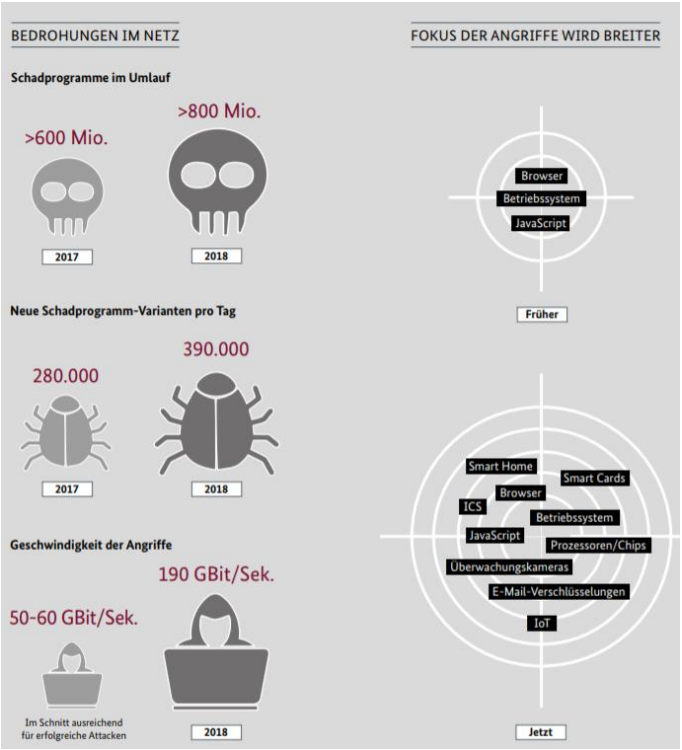
Telefon: +49 9431 7173 130
eMail: marketing@d-s.group

Gabelsbergerstraße 1
D - 92421 Schwandorf

Laut dem „Lagebericht zur IT-Sicherheit 2018“, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI), fanden Malware-Infektionen mit knapp 57 Prozent am häufigsten statt. Hacking-Angriffe machten 19 Prozent aus, DDoS-Attacken 18 Prozent.



Quelle: BSI-Dokument „Die Lage der IT-Sicherheit in Deutschland 2018“



Quelle: BSI-Dokument „Die Lage der IT-Sicherheit in Deutschland 2018“

Zunehmende Bedrohungen, weitreichende Schäden

Die Schäden können mittlerweile gigantisch und existenzbedrohend sein. Ob im Radio, TV oder in der Presse - inzwischen werden täglich Fälle vermeldet. Zudem werden CyberCrime Attacken zunehmend kommerzialisiert. Ein Geschäftsmodell der Zukunft liegt in Malware-as-a-Service, bei dem Laien Steuerserver und Schadsoftware mieten können.

Leider stagniert die Anzahl der Cyber-Attacken nicht, von einem Rückgang kann schon gar nicht die Rede sein. Jährlich ist ein Zuwachs zu verzeichnen, zugleich werden die Angriffsarten immer ausgefeilter und auch der Fokus der Angriffe wird breiter (siehe Grafik „Bedrohungen im Netz“ vom Bundesamt für Sicherheit in der Informationstechnik (BSI)). Laut dem BSI sind knapp 70 Prozent der Unternehmen und Institutionen in Deutschland in den Jahren 2016 und 2017 Opfer von Cyber-Angriffen geworden.

Kleinere Unternehmen meist leichtes Angriffsziel

Große Unternehmen stellen rein finanziell die interessanteren Angriffsziele dar, aber sie sind auch mit entsprechenden Abwehrmaßnahmen ausgestattet und erschweren Cyber-Kriminellen das Angriffsszenario.

Im Gegensatz dazu sind kleinere Unternehmen häufig unzureichend oder gar nicht gegen potentielle Angriffe geschützt. Sie werden damit zum leichten Angriffsziel, salopp formuliert: zum schnellen Hack für zwischendurch. Die daraus resultierenden Schäden legen in vielen Fällen ganze Unternehmen lahm, was wiederum zu immensen finanziellen Schäden führen kann. Aber auch die Reputation wird unter Umständen beschädigt, wenn man Kunden und Lieferanten für eine (un-)gewisse Zeit nicht mehr bedienen kann.

Die Ergebnisse einer Forsa-Befragung[1] aus dem Frühjahr 2018 zeigen folgendes auf:

Je kleiner das Unternehmen, desto…

…geringer wird das eigene Risiko eingeschätzt

…besser wird der eigene Schutz eingeschätzt

[1] https://www.gdv.de/resource/blob/32708/d3d1509dbb080d899fbfb7162ae4f9f6/cyberrisiken-im-mittelstand-pdf-data.pdf

Pressekontakt:

Inez Paulus
Abteilungsleiterin Marketing

Telefon: +49 9431 7173 130
eMail: marketing@d-s.group

Gabelsbergerstraße 1
D - 92421 Schwandorf

…schlechter ist der tatsächliche Schutz vor IT-Risiken

…anfälliger sind Unternehmen auch für mehrfache Cyberangriffe

Hausgemachte Sicherheitsbedrohungen.

In einigen Betrieben haben alle Mitarbeiter, oftmals aus Unwissenheit, einen sogenannten Administrator Account. Diese Mitarbeiter verfügen damit über viele Befugnisse unter Windows. So können Sie beispielsweise Passwörter zurücksetzen (auch von anderen Mitarbeitern), haben Zugriff auf sämtliche Daten (ebenfalls von anderen Mitarbeitern) und können ungeprüft alles installieren (Soft- und Hardware). Besonders Letzteres kann fatale Folgen haben, wenn „verseuchte“ Software auf dem Rechner landet.

Aber auch der sorglose Umgang mit USB-Sticks stellt ein offenes Tor für Angriffe dar.

Besonders gefährlich wird es, wenn Mitarbeiter in Bezug auf IT Sicherheit nicht geschult oder zumindest sensibilisiert werden. Dann ist die Gefahr groß, dass sogenannte Phishing eMails oder andere Bedrohungen nicht von Mitarbeitern erkannt werden.

1.2 Störungen des Betriebsablaufs durch technische Probleme

Bild: Pixabay

Vom kleinen Problem zum Totalausfall bedarf es manchmal nur eines falschen Klicks

Während der übliche Papierstau im Drucker noch problemlos von jedem Mitarbeiter alleine entfernt werden kann, können andere technische Probleme zur echten Herausforderung für Laien werden und in manchen Fällen sogar zum Totalausfall des IT Systems führen.

Bei einer defekten Festplatte zum Beispiel stellt die Bestellung einer neuen noch kein Problem dar. Nicht mehr ganz so trivial ist dann aber die Wiederherstellung von Daten, wenn diese (wodurch auch immer) beschädigt wurden.

Eines der wichtigsten Themen, um einen Totalausfall zu verhindern, stellt die Datensicherung (Backup) dar. Egal ob Daten physikalisch beschädigt wurden (Feuer, Wasserschäden, etc.), oder durch externe Angriffe zerstört oder gesperrt wurden - der wichtigste Rettungsacker ist immer ein funktionstüchtiges Backup. Damit lassen sich im Notfall alle Daten wiederherstellen, eine Weiterarbeit ist damit, je nach Datenumfang, relativ schnell wieder gewährleistet. So sinnvoll, so schwierig. Damit dieser Notfallplan auch funktioniert, bedarf es zum einen eines tiefergehenden Wissens, zum anderen muss in der Praxis dafür Sorge getragen werden, dass die Datensicherung regelmäßig durchgeführt wird. Darüber hinaus ist eine regelmäßige Überprüfung der Backup-Protokolle notwendig sowie Test-Rücksicherungen (Test Restores).

Sobald mehr als ein PC genutzt wird, ist ein Netzwerk in den meisten Fällen sinnvoll oder gar notwendig. Aber auch hier bedarf es grundlegenden Wissens, um alles richtig einzurichten und anfallende Probleme schnell zu lösen.

Die regelmäßige Wartung von IT Systemen darf nicht unterschätzt werden. Besonders das rechtzeitige Einspielen von (Sicherheits-) Updates tragen erheblich zur Steigerung der IT Sicherheit bei. Auch veraltete Betriebssysteme und Programme müssen rechtzeitig ausgetauscht werden, da sie vom Hersteller keine Updates und keinen Support mehr erhalten, und somit zu einem leichten Angriffsziel für Cyber-Kriminelle werden.

Wird einem Mitarbeiter übertragen, dies alles neben seiner Arbeit im Auge zu behalten, handelt man im Grunde genommen grob fahrlässig. Man nimmt damit potentielle IT (Sicherheits-) Risiken in Kauf, die dem eigenen Unternehmen schaden. Dies kann aber auch rechtliche Konsequenzen mit sich tragen.

Pressekontakt:

Inez Paulus
Abteilungsleiterin Marketing

Telefon: +49 9431 7173 130
eMail: marketing@d-s.group

Gabelsbergerstraße 1
D - 92421 Schwandorf

2. Die rechtlichen Folgen für die Geschäftsleitung

Egal an wen ein Geschäftsführer IT Aufgaben delegiert, im Schadensfall haftet nicht der Mitarbeiter, sondern die Geschäftsleitung - persönlich. Dies ist in diversen Gesetzen geregelt. Arbeitnehmer haften nur bei grober Fahrlässigkeit, oder wenn dem Unternehmen vorsätzlich Schaden zugefügt wurde.

„Je nach Schwere eines entstandenen Schadens, können empfindliche Strafen drohen. Bild: Pixabay

3. Externe IT Dienstleistungen für mehr Sicherheit im Unternehmen

Auch wenn das IT Budget gering ist, die Beauftragung eines professionellen, externen IT Dienstleisters rechnet sich in vielerlei Hinsicht. IT Experten kümmern sich um den Anwendersupport, die Wartung der IT Infrastruktur und um IT Sicherheitsfragen.

- Mitarbeiter können sich ausschließlich auf ihre eigentliche Arbeit konzentrieren
- Die IT wird durchgehend betreut - unabhängig von Mitarbeiterausfall durch Urlaub, Krankheit, Kündigung
- Erhöhung der Datensicherheit und der Ausfallsicherheit
- Vorhandene IT „Altlasten“ werden analysiert und beseitigt, zukünftige Probleme proaktiv vermieden
- Im Notfall stehen Spezialisten schnell zur Verfügung
- Durch das umfassende Know-how eines IT Dienstleisters können Prozesse optimiert und ein zukunftsfähiges IT-Konzept erstellt werden
- IT Kosten sind planbar und transparent
- Gesetzliche Auflagen werden erfüllt

In welchem Umfang ein externer IT Dienstleister in Anspruch genommen wird, hängt von vielen Faktoren ab und kann durch eine eingehende Beratung geklärt werden. Für kleinere Unternehmen ist es meist ausreichend, wenn die regelmäßige Wartung ausgelagert wird und bei technischen Problemen ein IT Spezialist auf Abruf bereitsteht. In solchen Fällen bietet sich ein Wartungsvertrag an, der keine monatlichen Fixkosten mit sich trägt, sondern die Leistungen bei Bedarf angefordert und abgerechnet werden.

4. IT Systemhäuser bieten attraktive Angebote

Einige IT Systemhäuser haben den Bedarf erkannt und bieten entsprechende Angebote an. Dabei sind sowohl die Konditionen, als auch die angebotenen Leistungen speziell auf die Belange und Anforderungen kleinerer Unternehmen ausgerichtet.

So bietet zum Beispiel die DS Deutsche Systemhaus GmbH mit der flex.Card ein umfangreiches Vorteilspaket an, das speziell für die Ansprüche kleiner Unternehmen konzipiert wurde. Mit einer flex.CARD können sich die Mitarbeiter sowie die Geschäftsleitung auf ihr Kerngeschäft konzentrieren und sich darauf verlassen, dass die dazu notwendige IT Infrastruktur störungsfrei läuft. Das Vorteilspaket beinhaltet einen professionellen IT Service zu stark vergünstigten Konditionen, einen Preisnachlass für eine bewährte Administrations-Lösung (flex.ADMIN) sowie drei umfangreiche kostenlose Gutscheine im Gesamtwert von 1.600,- €. Mit dieser kostengünstigen Lösung ist die Unternehmens IT in professionellen Händen.

Pressekontakt:

Inez Paulus
Abteilungsleiterin Marketing

Telefon: +49 9431 7173 130
eMail: marketing@d-s.group

Gabelsbergerstraße 1
D - 92421 Schwandorf

Über DS Deutsche Systemhaus GmbH

Die DS Deutsche Systemhaus GmbH ist seit über 20 Jahren ein erfahrenes IT-Systemhaus für Infrastrukturen, Managed und Cloud Services.

Die hochqualifizierten Mitarbeiter kennen die IT-Anforderungen mittelständischer Unternehmen und liefern passgenaue Lösungen. Spezialisiert auf Managed Services, unter anderem im IT-Infrastrukturumfeld und Cloud Computing liefert DS zukunftssichere Lösungen. Alle eigenen Cloud-Dienste erbringt das Systemhaus aus in Deutschland betriebenen Rechenzentren.

DS ist spezialisiert auf Lösungen auf Basis von Microsoft-Produkten und überzeugt mit professionellen Dienstleistungen rund um Hochverfügbarkeit, Virtualisierung, Microsoft System Center, Microsoft Terminalserver und Exchange Server. Auch zum Thema Videokonferenzen sind die DS-Spezialisten sehr gute Ansprechpartner. Darüber hinaus beschafft DS sämtliche erforderliche Soft- und Hardware zu fairen Preisen von namhaften Herstellern.

DS unterstützt seine Kunden auch als externer Dienstleister, der wahlweise dauerhaft oder bei Personalengpässen die IT-Infrastruktur in Betrieb hält. Und auch beim Planen durchaus komplexer WLAN-Infrastrukturen können sich Auftraggeber auf DS verlassen.

DS Homepage: www.deutsche-systemhaus.eu

Eine komplette Übersicht der DS Group erhalten Sie unter www.d-s.group

Pressekontakt:

Inez Paulus
Abteilungsleiterin Marketing

Telefon: +49 9431 7173 130
eMail: marketing@d-s.group

Gabelsbergerstraße 1
D - 92421 Schwandorf