Cyberbedrohungen als stetig wachsende Gefahr: Warum professioneller Schutz vor Ransomware mittlerweile für jedes Unternehmen unabdingbar ist

Schwandorf, 09.11.2021. Anfang dieses Jahres wurde laut Bundesamt für Sicherheit in der Informationstechnik (BSI) der bislang größte gemessene Schaden durch neuartige Schadsoftware (Malware) registriert[1]. Zu einer dieser Malware-Varianten zählt Ransomware, welche hauptsächlich Unternehmen betrifft. Mittlerweile geraten auch immer mehr Unternehmen aus dem Mittelstand in den Fokus der Kriminellen, mit teils existenzbedrohenden Folgen.

Doch was ist Malware bzw. Ransomware und welche Unternehmen sind genau betroffen? Besteht tatsächlich eine ernstzunehmende Gefahr? Wie können sich Unternehmen davor schützen? Die Antworten auf diese häufig aufkommenden Fragen sind erschreckend, aber zugleich einleuchtend.

Was versteht man unter Malware und Ransomware?
Malware (engl. „Schadsoftware“) ist der Überbegriff für jegliche Art von Schadprogrammen. Darunter fällt auch Ransomware, die eingesetzt wird, um sämtliche Daten des Opfers zu verschlüsseln, sodass der Nutzer keinen Zugriff mehr darauf hat. Durch eine Nachricht erhält man eine Lösegeldforderung, die eine Entschlüsselung nach erfolgreicher Zahlung (meist in virtueller Währung wie Bitcoin) verspricht. Eine Garantie, dass durch die Bezahlung tatsächlich eine Entschlüsselung erfolgt und nicht eine weitere Erpressung nach sich zieht, gibt es nicht. Die Angreifer drohen bei einer verspäteten oder nicht erfolgten Zahlung, die Daten für immer zu löschen - wobei seit neuestem sogar mit einer Veröffentlichung der sensiblen Daten gedroht wird.

Welche Unternehmen sind gefährdet?
Prinzipiell gilt: Unternehmen mit mangelnden Sicherheitsvorkehrungen ermöglichen den Cyberkriminellen ein leichtes Spiel und werden entsprechend oft bevorzugt. Faktoren wie die Unternehmensgröße oder -umsatz spielen bei der Auswahl fast keine Rolle – somit ist jede Firma potentiell der Gefahr von Ransomware-Angriffen ausgesetzt. Ein großer Irrtum ist der Glaube, dass keine Gefahr besteht, da keine wichtigen Daten vorhanden sind. Der Fehler: Jedes noch so kleine Unternehmen speichert Kundendaten, Rechnungen, Kontodaten, Mitarbeiterdaten etc. Sollten diese Daten durch einen Ransomware-Angriff verschlüsselt werden, so kann das Unternehmen nicht mehr darauf zugreifen. Aufträge können nicht abgewickelt, Rechnungen nicht erstellt, Bestellungen nicht abgegeben werden - um nur einige Beispiele zu nennen. Kurz: Nichts geht mehr - und das kostet in vielerlei Hinsicht Geld. Neben Betriebsausfallkosten und eventueller Schadensersatzforderungen kann unter Umständen auch eine Bußgeldzahlung hinzukommen. Schlimmstenfalls muss das geforderte Lösegeld bezahlt werden. Aber auch die Reputation eines Unternehmens kann langfristig durch einen Ausfall leiden.

Wurden zuvor keine Sicherheitsmaßnahmen getroffen, wie z.B. ein Backup der Daten, so bleibt manchmal der einzige Ausweg die Zahlung der Lösegeldforderung. Die Summe variiert von Fall zu Fall, ist aber meistens finanziell sehr belastend. Vor allem kleine und mittelständische Unternehmen können sich die geforderte Summe fast gar nicht leisten – somit stellt ein Cyberangriff bei unzureichender IT Sicherheit Unternehmen vor folgenschwere Probleme.

[1] Informationstechnik, B. f. (21. 10 2021). *BSI-Lagebericht 2021: Bedrohungslage angespannt bis kritisch*. Von BSI Bund: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/211021_Lagebericht.html

Pressekontakt:
Inez Paulus
Prokuristin
Telefon: +49 9431 7173 130
eMail: marketing@d-s.group
Gabelsbergerstraße 1
D - 92421 Schwandorf

Erschreckende Entwicklungen in Deutschland

Die Bitkom Studie 2021 kommt auf ein Ergebnis von 88 % aller deutschen Unternehmen, die von Malware-Angriffen betroffen sind bzw. waren. Dem AV-Test Institut zufolge hat sich die Anzahl an Malware seit 2016 mehr als verdoppelt – heute gibt es insgesamt etwa 1283,12 Millionen Schadprogramme und täglich kommen 450.000 neue Varianten hinzu. Dieser Anstieg spiegelt sich auch im Ausmaß der durch Angriffe entstandenen finanzielle Schäden wieder: Momentan spricht man in Deutschland von 223 Milliarden Euro wirtschaftlicher Schäden pro Jahr – im Vergleich zu 103 Milliarden Euro in 2018/2019 hat sich die Schadenssumme demnach auch hier mehr als verdoppelt. Neben finanziellen Schäden kommt es jedoch auch zu weiteren wirtschaftlichen Schäden, z.B. bei Produktionsprozessen, die teils existenzbedrohend sein können[2] [3]. Laut Ergebnissen der Bitdefender Labs liegt Deutschland mit 7 % an gefundener Ransomware weltweit auf Platz 5, die USA liegt im Vergleich mit 30 % auf dem ersten Platz [4].

Schutzmaßnahmen und Hilfe im Notfall

Wichtig ist es in erster Linie, sich vor Ransomware zu schützen. Präventions- und Schutzmaßnahmen sollten aufgrund der möglichen hohen immateriellen Schäden mit Sorgfalt ausgewählt werden. Natürlich können eigene Schutzmaßnahmen schon hilfreich sein. Doch hinsichtlich der teils existenzbedrohenden Schäden durch einen Ransomware Angriff, wird eine professionelle Beratung bei der Wahl der richtigen Ausstattung sowie eine sinnvolle und korrekte Integration dringend empfohlen. Die DS Deutsche Systemhaus GmbH unterstützt seit mehr als 25 Jahren Unternehmen im Ausbau der IT Sicherheit und gilt daher als kompetenter Ansprechpartner für IT Sicherheitsmaßnahmen.

Sollte dennoch (oder aufgrund fehlender Schutzmaßnahmen) ein Angriff erfolgt sein, gilt es, richtig zu reagieren, um die Auswirkungen so gering wie möglich zu halten und die IT Systeme schnellstmöglich wieder zum Laufen zu bringen. Für solch einen Notfall steht die DS Consult + Compliance GmbH mit einem international erfahrenen Expertenteam aus u.a. IT Security Spezialisten und IT Forensikern bereit. Sie ergreifen Sofortmaßnahmen zur Behebung bzw. Eingrenzung des Schadens und übernehmen die gesamte Dokumentation und Beweisführung. Dies und weitere Leistungen (auch zur Prävention) werden Unternehmen im Ernstfall geboten.

Live Webinar: „Achtung Ransomware: Prävention und Verhalten im Notfall“

Da die Theorie wie in den meisten Fällen stark von der Praxis abweicht, bietet die DS Deutsch Systemhaus GmbH deshalb im November ein kostenloses Live Webinar zum Thema „Achtung Ransomware: Prävention und Verhalten im Notfall“ an. Ziel ist es, den Teilnehmer:innen bestmögliches Praxiswissen zu vermitteln: Angefangen bei der ausgehenden Gefahr von Ransomware sowie den typischen Angriffswegen der Täter, gefolgt von Maßnahmen zum Schutz und Prävention. Im Falle eines tatsächlichen Angriffs wird auch das richtige Verhalten im Notfall thematisiert. Die Veranstaltung findet am 17.11. sowie am 24.11. online statt. Mehr Informationen und die Anmeldung ist im Internet unter https://www.deutsche-systemhaus.eu/veranstaltungen/ zu finden.

---

[2] Weber, A. (5. August 2021). *Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr*. Von Bitkom Research: https://www.bitkom-research.de/de/pressemitteilung/angriffsziel-deutsche-wirtschaft-mehr-als-220-milliarden-euro-schaden-pro-jahr

[3] *Malware*. (21. Oktober 2021). Von AV-TEST: https://www.av-test.org/de/statistiken/malware/

[4] Zugec, M. (29. September 2021). *Bitdefender Threat Debrief | August 2021*. Von Bitdefender: https://businessinsights.bitdefender.com/bitdefender-threat-debrief-august-2021

Pressekontakt:

Inez Paulus
Prokuristin

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 25 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
Prokuristin
Telefon: +49 9431 7173 130
eMail: marketing@d-s.group
Gabelsbergerstraße 1
D - 92421 Schwandorf