Die Gefahr von Ransomware

Sind die Daten in ihrem Unternehmen geschützt?

Was ist eigentlich Ransomware?

Es handelt sich um ein Schadprogramm, dass in den meisten Fällen durch Anhänge in Mailnachrichten in das Unternehmen gelangt. Ist das unternehmenseigene Netz erst einmal infiziert, beginnt die Software damit, die Unternehmensdaten derart zu verschlüsseln, dass ein Zugriff ohne den entsprechenden Schlüssel nicht mehr möglich ist. Oftmals erfolgt der Angriff erst Monate nach der Infektion, zwischenzeitlich hat die Verschlüsselungssoftware auch die Backups des Unternehmens befallen und schließt diese beim aktiv werden mit ein, in den Verschlüsselungsprozess. Kurz nachdem die Daten verschlüsselt sind, erhält man in der Regel eine Aufforderung zur Lösegeldzahlung. Erst nach der Zahlung erhält man den Schlüssel, um die Daten wieder lesbar zu machen – oder eben nicht.

Die Gefahr der Verschlüsselungstrojaner schwebt über jedem Unternehmen, egal ob es sich um ein Global Player oder Kleinunternehmen handelt. Jeder Unternehmer sollte sich ins Bewusstsein rufen, dass die Aufrechterhaltung des operativen Betriebes ohne Zugriff auf die Unternehmensdaten schlichtweg nicht oder nur mit erheblichen Schwierigkeiten möglich ist.

Wie kann ich mich gegen den Virus schützen?

Ein umfassender Schutz kann nur über eine Kombination von technischen und organisatorischen Schutzmaßnahmen erreicht werden. Selbstredend sollten geeignete Virenschutzprogramme sein, die im besten Fall von zwei unterschiedlichen Herstellern sind und automatisch geupdatet werden, so dass immer die neuesten Signaturen aktueller Viren bekannt sind. Dazu gehört ein funktionierendes Patchmanagement, wodurch die Aktualität der eingesetzten Soft- und Hardwareprodukte gewährleistet ist. Andernfalls besteht immer die Gefahr der Ausnutzung von bekannten Sicherheitslücken durch einen Hacker, wenn diese nicht rechtzeitig nach Bekanntwerden auf den Systemen geschlossen wurden.

Technische Schutzmaßnahmen können noch so ausgereift sein, die Gefahr, die vom Faktor Mensch als schwächstes Glied in der Security-Kette ausgeht, kann dadurch nicht beseitigt werden. **Eine regelmäßige Schulung und Sensibilisierung der Mitarbeiter, hinsichtlich der Gefahren von Schadprogrammen, ist unverzichtbar und muss als ebenso wichtig angesehen werden, wie ein funktionierender Virenscanner.** Ohne entsprechendes Problembewusstsein der IT-Benutzer wird früher oder später ein schadhafter E-Mailanhang angeklickt und der Schaden ist da.

Daneben sind noch viele weitere Faktoren maßgeblich, um ein angemessenes Sicherheitsniveau um Unternehmen zu erreichen. Oftmals fehlt der Unternehmensleitung allerdings die notwendige Übersicht über den aktuellen Status der Informationssicherheit, wir beraten Sie hier gerne umfassen.

Wie bin ich im Katastrophenfall richtig abgesichert?

Einen hundertprozentigen Schutz gegen die Bedrohung durch einen Verschlüsselungstrojaner zu erreichen ist nahezu unmöglich, da menschliches Versagen niemals auszuschließen ist und dieser Risikofaktor daher immer bestehen bliebt. Gegen den Eintritt des Katastrophenfalls müssen insofern bereits im Vorfeld ausreichend Maßnahmen getroffen werden, um gegen einen drohenden Datenverlust gewappnet zu sein.

Das einzige probate und **unerlässliche Mittel ist ein strukturiertes Backup-Konzept** zur Absicherung gegen Datenverluste. Das Unternehmen muss jederzeit in der Lage sein, verschlüsselte Daten innerhalb eines kurzen Zeitraumes wiederherstellen zu können. Bei der Erstellung eines umfassenden Datensicherungskonzeptes sind zahlreiche Faktoren zu beachten, wie Verfügbarkeitsansprüche, Lagerorte der Datenträger und Wiedereinspielungszeiten. Darüber hinaus muss das **Datenträgermanagement im eigenen Unternehmen** geregelt ablaufen, so dass jederzeit bekannt ist, wer über Speichermedien verfügt und wo diese eingesetzt werden. Es muss klar definiert werden, welche Daten zu welchen Zeitpunkten gesichert werden müssen und in wessen Verantwortungsbereich diese Aufgabe fällt.

Datensicherungen sollten grundsätzlich nicht über das Firmennetzwerk erreichbar sein und offline aufbewahrt werden, so dass sich Schadprogramme nicht auf bereits erstellte Backups übertragen lassen. Der Datensicherungsprozess muss als Routineaufgabe definiert werden, wozu, neben der täglichen Kontrolle des Sicherungserfolges, auch ein regelmäßiger Wiederherstellungstest durchzuführen ist, ob die Daten fehlerfrei auf die Systeme zurückgespielt werden können. Daneben gibt es noch viele weitere Parameter, die es zu beachten gilt für die Erreichung eines angemessenen Datensicherheitsniveaus.

Zur Feststellung des Sicherheitsniveaus empfiehlt es sich ein Datensicherungsaudit zu initiieren und im Anschluss eine grundsätzliche Prüfung der Risikolage hinsichtlich der Informationssicherheit im Unternehmen einzuleiten. Die Ausfallschäden, bei fehlender Zugriffsmöglichkeit auf die eigenen Daten, können mitunter existenzvernichtende Wirkung haben, insofern sollten angemessene Schutzmaßnahmen getroffen und nicht an der falschen Stelle gespart werden.

Wir beraten Sie gerne!

BT Nord Systemhaus GmbH

Stammsitz
Siemensstr. 28
25813 Husum
Fon +49 4841 89680

Niederlassung
Lise-Meitner-Str. 20
24941 Flensburg
Fon +49 461 16770020

Amtsgericht Flensburg I HRB 354 Husum

BT Nord Digital GmbH

Brandstwiete 46
20657 Hamburg
Fon +49 40 180245341

Amtsgericht Hamburg I HRB 165328 Hamburg

Geschäftsführer:
Thomas Holst CEO
Thies Kracht, Dipl.-Ing. (FH), CTO
Prokurist: Frank Thomsen

Umsatzsteuer-ID: DE134657285

Nord-Ostsee Sparkasse IBAN DE70 2175 0000 0186 0948 19 I BIC NOLADE21NOS
VR Bank Westküste eG IBAN DE70 2176 2550 0004 0133 36 I BIC GENODEF1HUM

www.btnord.de
info@btnord.de