Die Gefahr von Ransomware
Sind die Daten in ihrem Unternehmen geschützt?

Das Modul *Ransomware-Checkup* der BT Nord
Unter Ransomware versteht man Schadsoftware, die auf Verschlüsselung von Dateien spezialisiert ist, um diese unbrauchbar zu machen. Es werden jedoch nicht nur die lokalen Systeme befallen, sondern der Virus verbreitet sich wo immer auch Dateien zu finden sind, sogar teilweise auch gezielt auf Backups! Nach der Verschlüsselung wird das Opfer aufgefordert hohe Lösegelder zu zahlen, um den Schlüssel zu den Dateien zu erhalten.

In unserem Ransomware Checkup prüfen wir die Empfehlungen des Bundesinstituts für Sicherheit in der Informationstechnik (BSI) zu ebendieser Bedrohung, inwieweit notwendige Schutzmaßnahmen umgesetzt wurden in Ihrem Unternehmen.

Im Anschluss an die Prüfung erhalten Sie einen Bericht, in dem der Erfüllungsgrad in Prozent ausgegeben wird, die Mängel aufgezeigt werden und schließlich welche Maßnahmen zur Beseitigung der Mängel umzusetzen sind. Im Rahmen einer Abschlussbesprechung sollten gemeinsam Maßnahmen priorisiert werden, die ein sehr hohes Risiko für das Unternehmen darstellen. Auf Basis des Berichts kann die Geschäftsführung notwendige Entscheidungen treffen zur Umsetzung, ohne umfassende technische Kenntnisse zu besitzen.

Ziel des Ransomware-Checkups

- IST-Analyse zum Thema Sicherheit gegen Ransomware
- Prüfung der Vorgaben des BSI durch Checklisten-Tool ITQX
- Automatische Berichtserstellung
- Werkzeug als Basis für Optimierungen
- Maßnahmenplan zur Abstellung von Mängeln
- Mess- und Führungsinstrument für Geschäftsleitung/IT
- Sensibilisierung
- Schwachstellen konkret benennen

BT Nord Systemhaus GmbH
Siemensstr. 28, 25813 Husum
+49 4841 89680
info@btnord.de
www.btnord.de

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

Amtsgericht Flensburg
HRB 354 HU

Umsatzsteuer-ID:
DE134657285

Bankverbindungen:
Nord-Ostsee Sparkasse
BIC: NOLADE21NOS
IBAN: DE70 2175 0000 0186 0948 19

VR Bank Westküste eG
BIC: GENODEF1HUM
IBAN: DE70 2176 2550 0004 0133 36

Wie kann ich mich weiter gegen den Virus schützen?
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-Mail-Anhang 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.

BT Nord Systemhaus GmbH
Siemensstr. 28, 25813 Husum
+49 4841 89680
info@btnord.de
www.btnord.de

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

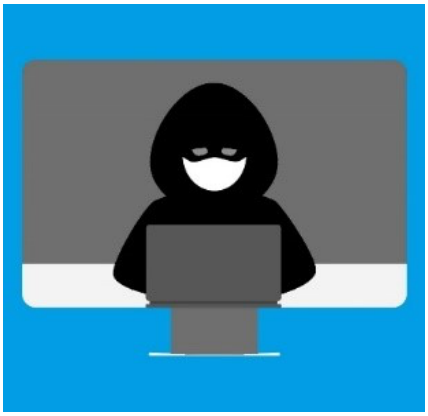
Amtsgericht Flensburg
HRB 354 HU

Umsatzsteuer-ID:
DE134657285

Bankverbindungen:
Nord-Ostsee Sparkasse
BIC: NOLADE21NOS
IBAN: DE70 2175 0000 0186 0948 19

VR Bank Westküste eG
BIC: GENODEF1HUM
IBAN: DE70 2176 2550 0004 0133 36

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
Siemensstr. 28, 25813 Husum
+49 4841 89680
info@btnord.de
www.btnord.de

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

Amtsgericht Flensburg
HRB 354 HU

Umsatzsteuer-ID:
DE134657285

Bankverbindungen:
Nord-Ostsee Sparkasse
BIC: NOLADE21NOS
IBAN: DE70 2175 0000 0186 0948 19

VR Bank Westküste eG
BIC: GENODEF1HUM
IBAN: DE70 2176 2550 0004 0133 36