```
Damage Your Files Permanently (...)
```

Ferner sind in den Dateien Anweisungen enthalten, dass

- Beispieldateien zur testweise Entschlüsselung übersendet werden sollten,
- Bitcoins zu beschaffen sind (einschließlich Informationen, wie man diese kaufen kann),
- man gegen Zahlung einer noch zu bestimmenden Summe die Entschlüsselung vornehmen werde.

A zieht sofort die betreuenden Mitarbeiter von E hinzu. Sie stellen fest, dass die regulären Backups auf Netzlaufwerken ebenfalls entweder verschlüsselt oder zumindest beschädigt sind. Diese seien notwendigerweise im Netzwerk verfügbar gewesen, weil sie bei Erstellung von Backups (nachts) automatisch eingebunden wurden. Im Unternehmen kann man ab sofort nicht mehr arbeiten - es entgeht pro Arbeitstag ein Umsatz in Höhe von ca. 50.000,- EUR, während kaum Kosten gespart werden können. Zahlreiche Aufträge für die Kunden können bei einem Ausfall länger als eine Woche nur verzögert abgewickelt werden.

Sollten die Daten nicht entschlüsselt werden, sind Daten der letzten 3 Monate verloren - so alt ist das letzte intakte Backup von einem stillgelegten Computer. Können neuere Daten nicht wiederhergestellt werden, sind die laufenden Projekte des Unternehmens um mindestens jeweils 40 Arbeitstage zurückgeworfen, mit der gleichen Folge für die Fertigstellung der Projekte. Die Arbeitszeit im Wert von ca. 2.000.000,- EUR geht verloren, eine weitere Million ist insgesamt für Vertragsstrafen zu erwarten.

Ein externer Berater wird hinzugezogen und stellt Folgendes fest:

- die auf Windows Server 2016 basierende Infrastruktur (Active Direktory, Netzlaufwerke) wurde kompromittiert,
- ein Rechner im Netzwerk (Windows 10 Pro) wurde durch Mitarbeiter der E zu Wartungszwecken mit aktivem RDP-Dienst betrieben,
- im Router und in der Firewall von A wurde eine entsprechende Weiterleitung zu diesem Wartungsgerät eingerichtet,
- die Mitarbeiter von E haben zwar ein Mapping des Ports (Port 51888 von außen auf 3389 intern) vorgenommen, aber dennoch war der RDP-Port 3389 auf einem Umweg von außen zugänglich,
- höchstwahrscheinlich wurde in den Wartungsrechner über eine //brute-force//-Attacke eingebrochen;
- von dort aus hatte Schadsoftware ein leichtes Spiel, das komplette Netzwerk von A zu kompromittieren, weil die Netzwerkfreigaben zwar mit einem durchdachten Rechtesystem versehen, dennoch immer auch Freigaben ohne Zugriffsschutz vorhanden waren, über die die Infektionen weiterer Rechner begannen;
- der Zugriff erfolgte bereits ca. 2 Wochen vor den erkennbaren Problemen, die Verschlüsselung startete am Freitag, 18. 9.,
- die Schadsoftware, die eingesetzt wurde, ist eine neue Variante einer bereits bekannten Verschlüsselungsattacke und deshalb konnte sie auch Systeme mit allen verfügbaren Sicherheitsupdates befallen,

- die Schadsoftware durch Antivirus-Programm auch nach Attacke und bei gezielter Suche nicht als solche erkannt wurde.

a. Wie gehen Sie vor? Soll das Lösegeld gezahlt werden?

b. Wie sichern Sie sich gegen einen derartigen Angriff ab?

3. Szenario 3: Vorbereitung auf einen Zwischenfall

Das Unternehmen U, das mit Möbelproduktion und Handel ca. 20 Mio. EUR Umsatz jährlich erwirtschaftet und etwa 50 Mitarbeiter beschäftigt, wurde bereits mehrfach Opfer kleiner Cyberangriffe. Es war auch - wegen einiger Besonderheiten der von U genutzten IT-Infrastruktur - einige Male von technischen Ausfällen betroffen, auch wenn größere Schäden bisher vermieden werden konnten.

Die Geschäftsleitung stellt fest, dass die in anderen Unternehmen bereits vorgekommenen Daten-GAUs für U das sprichwörtliche "Genickbruch" bedeuten könnten. Um sich auf diesen Fall vorzubereiten und erheblichen finanziellen Schaden abzuwenden, möchte die Geschäftsleitung eine sog. Cyber-Versicherung abschließen. Die angefragte Versicherungsgesellschaft ist bereit, eine zufriedenstellende Absicherung anzubieten, allerdings unter der Bedingung eines ausführlichen Audits und Anpassung der IT-Landschaft von U an "best practices" gemäß Vorgabe der durch die Versicherung benannten IT-Experten. Diesen Weg wollen die Geschäftsführer von U gehen.

Im ersten Gespräch mit den Beratern wird deutlich, dass die Kosten des Audits und der Beratung enorm sein werden. Sie lassen sich aber deutlich reduzieren, wenn sich U auf den Audit intern gut vorbereitet und grundlegende Maßnahmen bereits vor dem Audit vorbereitet bzw. umsetzt. In diesem Fall können die Berater Vollzug bestätigen, ohne dass hohe Kosten anfallen

Sie arbeiten bei U und sollen nun Ihr Wissen über den Umgang mit Daten- und IT-Sicherheit einbringen. Die Geschäftsleitung bittet Sie, "alles Notwendige" zu unternehmen.

Was ist zu tun?