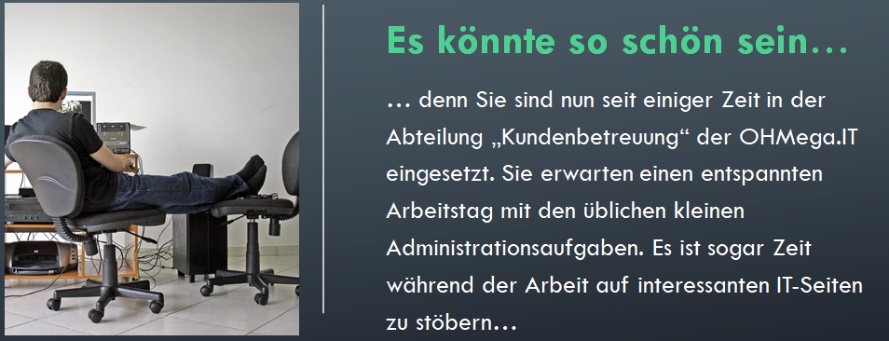
# Szenario

Doch dann…

**Plötzlich erleben Sie Ihren Chef aufgewühlt:** Einer ihrer Neukunden, die Steuerberatung „Unglück & Partner GbR“, hat eine erschütternde Email geschrieben:

*Hallo Ohmega-IT,*

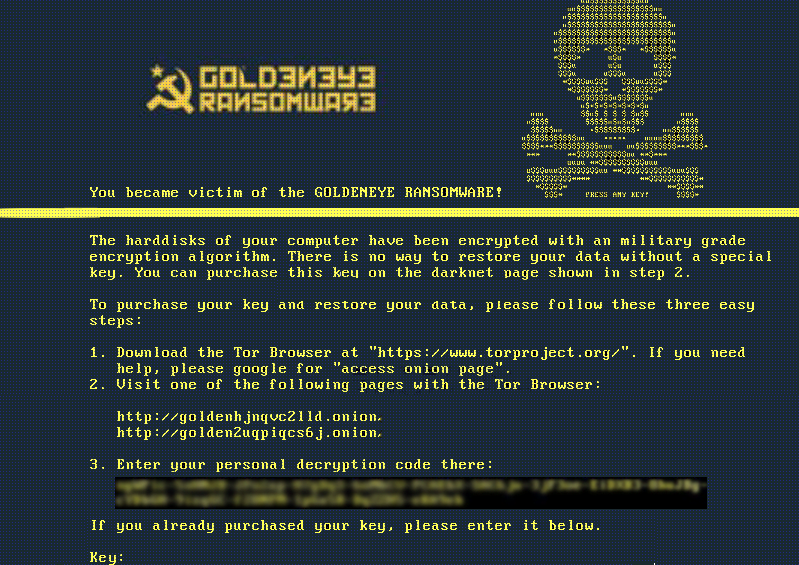
*leider müssen wir heute morgen feststellen, dass alle unsere Arbeitsplätze nicht mehr funktionieren!!! Wir können uns nicht mehr anmelden, auch die Heimarbeitsplätze gehen nicht mehr.*

*Auf dem Bildschirm des Servers erscheint eine unmissverständliche Nachricht. Immer wieder haben wir in der Vergangenheit gehört, dass Firmen angegriffen werden und man Bitcoins fordert, aber wir hätten nie gedacht, dass wir als Ziel in Frage kommen!*

*Da Sie ja erst seit 4 Wochen unsere neue IT-Firma sind, ist uns ist schon klar, dass das nicht in ihrer Verantwortung liegt, aber helfen Sie uns! Unser ganzer Betrieb steht still!*

*Hier noch ein Screenshot vom Server, war müssen wir jetzt tun?  
Danke und bitte dringend!*

*Ulrich Unglück*



**Was nun?**

Ihr **erfahrener Chef**, Herr Dümpelfeld, ist schon auf dem Weg zum Kunden und wird sich vor Ort um die technischen Aspekte kümmern. Schließlich war schon bei der Übernahme des Services klar, dass bei „Unglück & Partner“ **einiges im Argen** liegt…

**Sie** hingegen sollen dringend klären, wie die **Gesetzeslage** aussieht. **Müssen Sie den Vorfall melden?** Was ist überhaupt nun alles zu tun? Die ganzen Statistiken der Sicherheitsvorfälle und die Seiten des BSIs erscheinen Ihnen plötzlich in einem anderen Licht…

# Aufgabe:

Beantworten Sie die folgenden Fragen mit dem Material (AB3B) des BSI! Es geht dabei weniger um Ihre (spannende) Ersteinschätzung als um das, was das BSI dazu empfiehlt.

* Bei den *kursiven Passagen* müssen Sie sich **entscheiden** welche Aussage richtig ist. (unterstreichen / fettdrucken)
* Hinter den **…** müssen Sie die Aussage **vervollständigen**, z.B. eine Begründung angeben. Bitte **gründlich** und im ganzen Satz.

Viel Erfolg!

# Organisatorische und technische Maßnahmen beim IT- Sicherheitsvorfall

#### Organisatorische Aspekte

1. Zunächst müssen Sie dafür sorgen, dass der IT-Sicherheitsvorfall ***vorrangig* *nach innen*** */ ~~vorrangig~~**~~nach außen~~* bekannt gemacht wird. Dazu müssen folgende Personen davon erfahren: … **die Geschäftsführung, die IT-Abteilung und die Rechtsabteilung.**
2. Eine Schadanalyse kann der erste Schritt bei der Bewältigung des Vorfalls sein. Sie soll klären, **die Art, den Umfang und die Ursache des Sicherheitsvorfalls zu einschätzen.**
3. Die kurzfristige Wiederherstellung der Arbeitsfähigkeit ist *~~zunächst erstmal keine Zeit~~ /* ***nachrangig*** */ ~~leider nicht möglich~~*, weil **zunächst die Eindämmung erfolgen soll.**
4. Hinsichtlich der Meldepflicht ist die Gesetzeslage der beiden Gesetze **Telemediengesetz** und **Bundesdatenschutzgesetz** zu beachten.
5. Der vorliegende IT-Sicherheitsvorfall ist *~~meldepflichtig~~ /* ***nicht meldepflichtig***, *weil* **es von verschieden Faktoren abhängig ist.**
6. Wenn Meldepflicht besteht, ist der Vorfall zu melden bei **der zuständigen Aufsichtsbehörde.**
7. Wenn Meldepflicht besteht, ist der Vorfall *~~sofort~~ / ~~binnen 24h~~ /* ***binnen 72h*** */ ~~einer Woche~~* zu melden, weil dieser Zeitraum **noch akzeptabel ist.**
8. Bei der Polizei ist *~~sofort~~ /* ***ggfs, später*** */ ~~nicht~~* ~~Anzeige~~ zu erstatten, weil **es möglich ist den Täter ggf. noch zu ermitteln.**
9. Die Einrichtung eines Krisenstabs ist ***überflüssig*** */ ~~nötig~~*~~,~~ *~~weil~~ /* ***obwohl*****man damit die Koordination besser organisieren kann.**
10. Wenn ein Krisenstab nötig ist, soll er die folgenden Personen und Gruppen enthalten: **die Geschäftsführung, die IT-Abteilung, die Rechtsabteilung, den Datenschutzbeauftragten, ggf. Vertreter von externen Dienstleistern und ggf. Vertreter von Behörden.**
11. Das Einschalten eines externen IT-Sicherheitsdienstleisters *ist vorgeschrieben / ~~wäre im vorliegenden Fall später immer noch möglich~~ /* ***wird vom BSI empfohlen***, wenn **der interne Sachverstand nicht ausreicht oder wenn eine schnelle und unabhängige Untersuchung des Vorfalls erforderlich ist.**
12. Die Behandlung des Sicherheitsvorfalls ist gegenüber dem Tagesgeschäft *~~zunächst zurückzustellen~~ /* ***sofort anzugehen***, weil … **die Behandlung eines IT-Sicherheitsvorfalls gegenüber dem Tagesgeschäft Priorität haben sollte**
13. Vom BSI ist im vorliegenden Fall *~~direkte Unterstützung~~ / ~~keine Hilfe~~ /* ***nur eingeschränkte Unterstützung***zu erwarten, weil **die Unterstützung nach Art des Vorfalls variieren kann.**
14. Nach Empfehlung des BSI soll der Lösegeldforderung grundsätzlich *~~umgehend (damit eine Entschlüsselung möglich bleibt)~~ /* ***nicht* eingegangen werden**, weil **es Kriminalität fördert, es nicht garantiert, es Rechtsfolgen mitziehen kann.**
15. Die Höhe der Lösegeldforderung lässt sich oftmals *~~nach geschickter Verhandlungen mit den Erpressern~~ / ~~nach Meldung an das BSI und die Presse~~ / ~~Einschaltung von IT-Sicherheitsdienstleistern~~ / ~~durch Offenlegung im Darknet~~* reduzieren.
16. Nach erfolgreicher Entschlüsselung der Daten müssen die Systeme *~~alle neu installiert~~ /* ***können die meisten Systeme weiterverwendet***werden, weil **Moderne Ransomware-Varianten verschlüsseln in der Regel nur die Daten, aber nicht die Betriebssysteme oder die Hardware der betroffenen Systeme.**
17. Nach dem IT-Sicherheitsvorfall sind weitere langfristige Maßnahmen zu ergreifen, damit **sich ein solcher Vorfall nicht wiederholen kann.**

#### Technische Aspekte:

1. Wenn **aktuelle Backups** vorhanden sind, *~~sollte sofort~~ /* ***sollte nicht sofort*** mit dem Wiedereinspielen der Daten begonnen werden, weil… **erstmal sichergestellt werden sollte, dass die Ransomware vernichtet wurden, ist.**
2. Ist nur ein **einzelnes** **System** auffällig, **sollte dieses vom Netz genommen** / ~~unbedingt am Netz behalten~~ werden, weil … **dieses sich sonst auf andere Systeme übertragen könnte.**
3. Wenn nur ein einzelnes System auffällig ist, ***kann*** */ ~~sollte nicht~~* mit den anderen Systemen weitergearbeitet werden, wenn das noch möglich ist, weil … **man nicht auf eine infizierte Maschine arbeitet.**
4. Es sollte zunächst **möglichst *nicht-invasiv analysiert werden****, ~~möglichst sofort ein~~* ***~~Neustart aller Systeme~~*** *~~durchgeführt~~* ~~werden~~, bevor gehandelt wird, weil … **es einen Payload erzeugen kann, welches sich dann auf andere Systeme verbreitet.**
5. Angreifer haben womöglich **Brückenköpfe** angelegt. Dabei handelt es sich um … **Stellung, die strategisch besser für die Angreifer sind!**
6. Ist der Brückenkopf beseitigt, ist die weitere Kommunikation des Angreifers ***unterbunden*** *~~/ nicht unterbunden~~,* weil … **die strategische Stellung beseitigt worden ist.**
7. Ist auf einem betroffenen System noch eine Anmeldung mit **privilegierten Konten** (Admin) möglich, sollte darüber das Konto des Angreifers umgehend gelöscht werden. ***Stimmt*** */~~stimmt nicht~~, weil …***noch Gefahr besteht, dass dieses benutzt, wird vom Angreifer.**
8. Das BSI empfiehlt, eine „**forensische Sicherung** incl. Speicherabbild des infizierten Systems“ zu machen. Das ist ein **Schutz** .... Und es dient dazu, dass … **man dieses als Beweismittel aufbewahrt.**
9. Nach der forensischen Sicherung soll das System neu ~~gestartet~~ / **heruntergefahren** / ~~hart ausgeschaltet~~ werden, weil … **es heißt Schadensreduzierung**
10. Virtuelle Systeme lassen sich ***leichter*** */ ~~komplizierter~~* forensisch sichern als physische, weil … es ein abgeschottetes System ist.
11. Das BSI empfiehlt, in **Logfiles** nach „http-Datenverkehr zu **Command & Control Servern**“ zu suchen. Was sind das für Server? …
12. Die Analyse der Logdateien *kann leicht / sollte nicht* vom Administrator der Firma durchgeführt werden, weil …
13. Das BSI empfiehlt, im Vorfeld auf der Firewall ein „**Full-Packet-Capturing**“ zu etablieren. Dabei handelt es sich um ein …, das problematisch sein kann, weil …
14. Das BSI spricht häufig vom „**AD**“, das ist das Active Directory. Das ist …
15. Ein Befall des AD ist als *weniger kritisch (da sich die Nutzer oftmals noch anmelden können) / äußerst kritisch* zu betrachten, weil …
16. Idealerweise sollten alle kompromittierten Systeme *schrittweise / zur gleichen Zeit* vom Netz genommen werden, weil …
17. Danach können die Systeme schrittweise neu gestartet und **Datei-Backups eingespielt** werden, damit weiter gearbeitet werden kann. *Stimmt /stimmt nicht, weil …*
18. Um Angriffe in Zukunft zu verhindern, muss – neben technischen Maßnahmen – auch mit zeitgemäßen **Rechte- und Password-Richtlinien** gearbeitet werden. *Stimmt /stimmt nicht.*

Dann hoffen wir mal, dass Ihr Chef, Herr Dümpelfeld, das alles in der richtigen Reihenfolge und auch schnell hinbekommt, halten Sie ihm die Daumen!