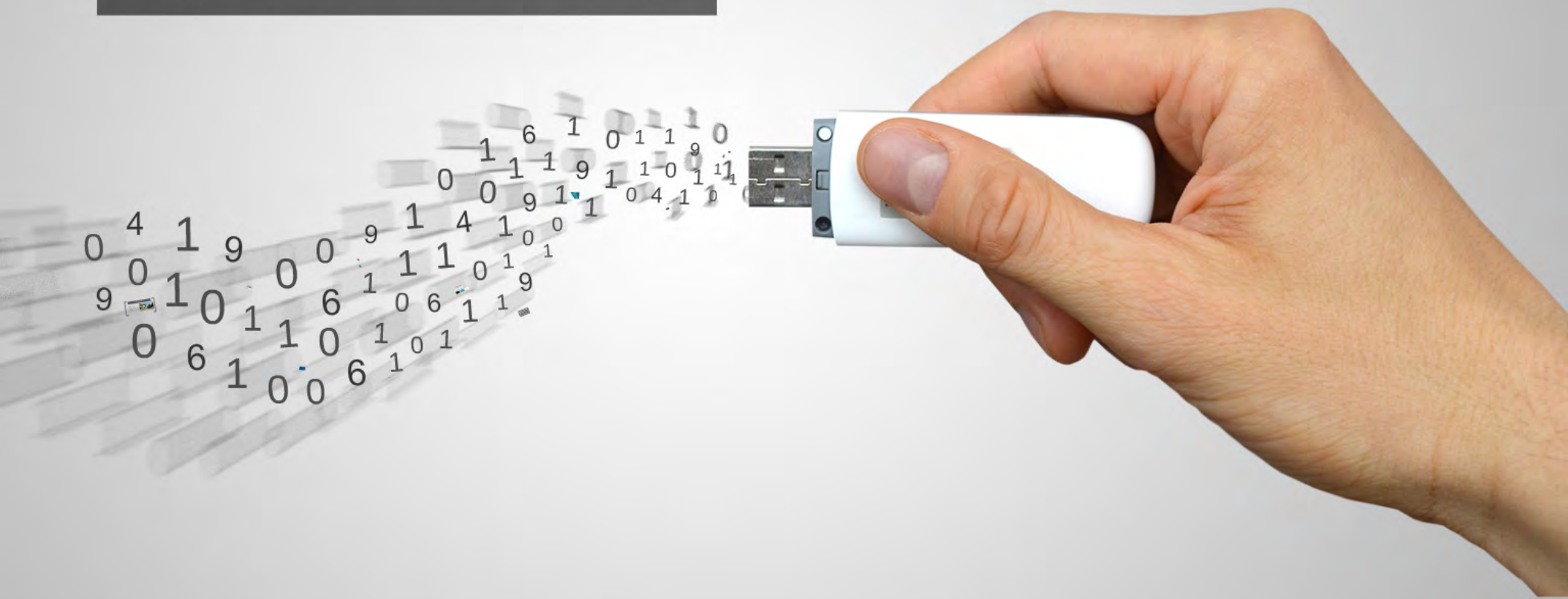


Cybersecurity



Vernetzung von Kommunen



E-government als Informations- und Kommunikationsraum für Politik



Administrative Leistungen des Staates können schneller und effizienter durchgeführt werden



Politische Meinungsäußerung ist leichter (z. B. durch Diskussionen in Foren, Möglichkeit zur Anonymität usw.)



Distanz zum Bürger ist geringer
(z. B. durch Politiker-Profile in sozialen Netzwerken)



“

Es gibt zwei Arten von Unternehmen: solche, die schon **gehackt wurden**, und solche, **die es noch werden.**

Robert Mueller, Direktor des FBI



Wer greift Unternehmen heutzutage an?

Cyber-Kriminelle

versuchen mithilfe von Cyberangriffen illegal Geld zu erbeuten.

Geheim- und Nachrichtendienste

Teilweise staatlich organisierte Wirtschaftsspionage.

Hacktivismus

Diese nutzen Cyberattacken für politische Meinungsäußerungen.

Interne Täter

Häufig Mitarbeiter, die sich übergangen/falsch behandelt fühlen.

Kommunale Webseite

Schadenszenario

Ein Webseite wurde Opfer einer Denial-of-Service-Attacke. Die Bürger konnten 48 Stunden lang nicht mehr drauf zugreifen.

Schadenbild

- Plötzlicher Anstieg des eingehenden Datenflusses
- Allmähliche Überlastung führt zur Nichtverfügbarkeit der Webseite
- Der Datenfluss wird nach Bekanntwerden analysiert und gefiltert
- Schrittweise Rückkehr zum Alltagsgeschäft (48 Std.)

Auswirkungen

- | | |
|--|----------|
| • Einsatz des internen IT-Teams | 35.000 € |
| • Externe IT-Mitarbeiter müssen helfen | 24.500 € |

Summe: 59.500 €

E-Mail Versand

Schadenszenario

In einer Stadtverwaltung wurde versehentlich eine Mail mit 200 sensiblen Kundendaten an eine falsche Mailadresse geschickt.

Schadenbild

- Mitarbeiter hat die Autovervollständigung im Outlook nicht geprüft
- Es wurde die Mail an einen aussenstehenden Dritten verschickt
- Das Thema war 2 Wochen in diversen Medien

Auswirkungen

- Kosten für IT-Forensik
- Rechtsberatung
- Informationspflicht

13.000 €

40.000 €

15.000 €

Summe: 68.000 €

Welche Daten müssen geschützt werden?

Gem. §3 Abs. 1 BDSG

- Namen und Adressen
- Fotos
- E-Mailadressen und Internet-Adresse
- Titel, Geschlecht, Größe, Haarfarbe, usw.
- Telefonnummer
- Personalausweisnummer
- Sozialversicherungsnummer

Gem. §9 BDSG "Sensible Daten"

politische Meinungen

Religionszugehörigkeit

Gewerkschaftszugehörigkeit

Gesundheitszustand

Sexualleben, z.B. Homosexualität

Haftung von Kommunen

Unternehmen, denen sensible Daten gestohlen wurden, müssen Behörden und Betroffene gem. **§42a BDSG** über die Datenschutzverletzung informieren.

Gem. **§ 7 und 8 des Bundesdatenschutzgesetzes** hat der Betroffene das Recht auf Schadensersatz. Daraus leitet sich auch das Recht auf eine Rechtsberatung ab.

Wichtig: "**unabhängig von einem Verschulden zum Schadenersatz verpflichtet.**"

IT - Sicherheitsgesetz

Betreiber Kritischer Infrastrukturen aus den Bereichen **Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung** sowie Finanz- und Versicherungswesen müssen damit künftig einen Mindeststandard an IT-Sicherheit einhalten.

Die verschlüsselte Stadt, die zahlte

Die **Computer** einer unterfränkischen Stadt sind durch Ransomware lahmgelegt worden. Die Verantwortlichen entschieden sich, die geforderten **Bitcoin** zu zahlen - mit Hilfe einer "Fachfirma".

Am 8. Februar ist die Stadtverwaltung der unterfränkischen Stadt Dettelbach mittels eines Erpressungstrojaners angegriffen worden - alle Daten wurden verschlüsselt. Um die Daten wieder zu entschlüsseln, sollte die Stadt 1,3 Bitcoin zahlen, derzeit etwa 500 Euro, [wie Spiegel Online berichtet](#). [↗](#) Dettelbach mit rund 7.000 Einwohnern liegt in der Nähe von Würzburg.

ANZEIGE

Die Polizei und das Bundesamt für Sicherheit in der Informationstechnik (BSI) raten davon ab, solche Erpressungssummen zu zahlen - erstens sei nicht sichergestellt, dass die Daten wieder freigegeben würden, zweitens würden die Kriminellen so ermutigt, weiterzumachen. Doch die Stadt entschied sich trotzdem zur Zahlung.

Wie kommt eine Stadtverwaltung an Bitcoin?

Das Problem: Wo bekommt die Verwaltung einer Kleinstadt Bitcoin her? In der Gemeindekasse liegen die sicher nicht. Aus diesem Grund habe die Stadt eine "Fachfirma" mit der Abwicklung der Zahlung beauftragt, bestätigte die Polizei Spiegel Online.

Dettelbach infizierte sich nicht mit dem derzeit grassierenden Locky-Trojaner, sondern mit Tesla-Crypt in der Version 2.0 oder 3.0. Die IT-Probleme wurden mit der Zahlung nicht vollständig behoben. Es sei zu einem "weitreichenden Ausfall des EDV-Systems mit Datenverlusten" gekommen, erklärte die Stadtverwaltung laut Spiegel Online. Diese Probleme seien durch "Fehlfunktionen im bestehenden EDV-System sowie Fehlentscheidungen bei der Rücksicherung" entstanden.

Das Einwohnermeldeamt der Stadt wurde zwischenzeitlich geschlossen. Ab Montag soll alles wieder wie gewohnt funktionieren. Nur die Stadtwerke sind mit ihrer Rücksicherung noch nicht ganz fertig. Wenn Kunden umziehen oder kündigen, sollen sie die Abrechnungen des vergangenen Jahres einschicken - sicherheitshalber in Papierform. ■

Die verschlüsselte Stadt, die zahlte

Die [Computer](#) einer unterfränkischen Stadt sind durch Ransomware lahmgelegt worden. Die Verantwortlichen entschieden sich, die geforderten [Bitcoin](#) zu zahlen - mit Hilfe einer "Fachfirma".

Am 8. Februar ist die Stadtverwaltung der unterfränkischen Stadt Dettelbach mittels eines Erpressungstrojaners angegriffen worden - alle Daten wurden verschlüsselt. Um die Daten wieder zu entschlüsseln, sollte die Stadt 1,3 Bitcoin zahlen, derzeit etwa 500 Euro, [wie Spiegel Online berichtet](#). [↗](#) Dettelbach mit rund 7.000 Einwohnern liegt in der Nähe von Würzburg.

ANZEIGE

Die Polizei und das Bundesamt für Sicherheit in der Informationstechnik (BSI) raten davon ab, solche Erpressungssummen zu zahlen - erstens sei nicht sichergestellt, dass die Daten wieder freigegeben würden, zweitens würden die Kriminellen so ermutigt, weiterzumachen. Doch die Stadt entschied sich trotzdem zur Zahlung.

Wie kommt eine Stadtverwaltung an Bitcoin?

Das Problem: Wo bekommt die Verwaltung einer Kleinstadt Bitcoin her? In der Gemeindekasse liegen die sicher nicht. Aus diesem Grund habe die Stadt eine "Fachfirma" mit der Abwicklung der Zahlung beauftragt, bestätigte die Polizei Spiegel Online.

Gesamtschaden über 100.000 € Dettelbach infizierte sich nicht mit dem derzeit grassierenden Locky-Trojaner, sondern mit Tesla-Crypt in der Version 2.0 oder 3.0. Die IT-Probleme wurden mit der Zahlung nicht vollständig behoben. Es sei zu einem *"weitreichenden Ausfall des EDV-Systems mit Datenverlusten"* gekommen, erklärte die Stadtverwaltung laut Spiegel Online. Diese Probleme seien durch "Fehlfunktionen im bestehenden EDV-System sowie Fehlentscheidungen bei der Rücksicherung" entstanden.

Das Einwohnermeldeamt der Stadt wurde zwischenzeitlich geschlossen. Ab Montag soll alles wieder wie gewohnt funktionieren. Nur die Stadtwerke sind mit ihrer Rücksicherung noch nicht ganz fertig. Wenn Kunden umziehen oder kündigen, sollen sie die Abrechnungen des vergangenen Jahres einschicken - sicherheitshalber in Papierform. ■

Oberflächenweb



Verborgenes Web

Internetseiten die nicht durch google gefunden werden, z.B.
Medizindatenbanken, Wissenschaftliche Daten, interne Bereiche, ...

Darknet



Phishing Mails

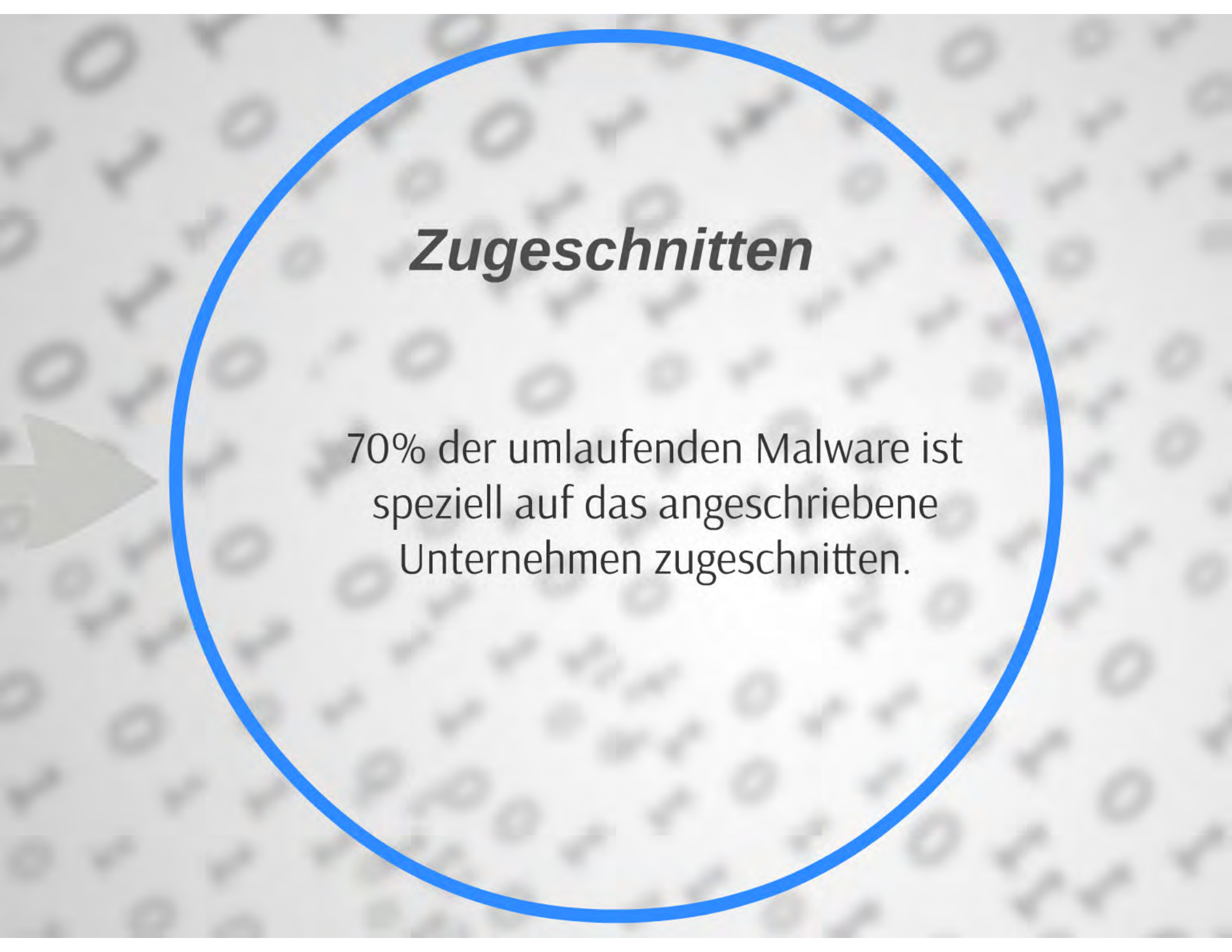
23% aller Empfänger von
Phishing-Mails öffnen
diese sofort und **11%**
öffnen auch den
Anhang.





Link in der Mail

50% aller Empfänger öffnen
und klicken auf einen Link in
der Mail innerhalb der ersten
Stunde



Zugeschnitten

70% der umlaufenden Malware ist
speziell auf das angeschriebene
Unternehmen zugeschnitten.

GEFAHREN

verwundbarer Systeme



FINANZAMT



ENERGIEVERSORGUNG



TOURISMUS



ZULASSUNGSSTELLE



RATHAUS



ENERGIEVERSORGER



SCHULEN UND UNIVERSITÄTEN



BAUHÖFE

Umgang mit den Risiken



Mitarbeiter

Wissen

Ein Mindestwissen zum Thema IT-Sicherheit muss vorhanden sein.

Sensibilität

Alle Beteiligten sollten eine gewisse Sensibilität an den Tag legen.

Mobile Geräte

Private Geräte sollten nicht ins Firmennetzwerk kommen.

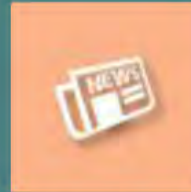
Internetzugang

Auf den Firmenrechner sollten keine privaten Mails gelesen werden.

Fremd- und Eigenschäden sind abgesichert.



Betriebsunterbrechung



Informationskosten



IT-Forensik



Kreditkarten-
überwachung



Krisen-
management



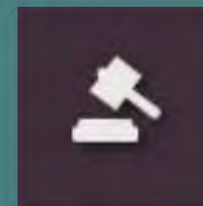
Haftpflicht



PR-Beratung



Rechtsberatung



Vertrauensschäden

Internet abschalten

**Scheibe einschlagen
Knopf tief drücken**

