Bayerisches Landesamt für
Datenschutzaufsicht

Mehr Datenschutz - bessere Cybersicherheit

Reaktion und Prävention am Beispiel Ransomware

Dorit Buschmann
Referentin im BayLDA
Bereich „Cybersicherheit und technischer Datenschutz“

Wer steht heute vor Ihnen?

Dorit Buschmann

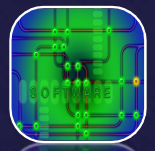
Referentin beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA)

Bereich „Cybersicherheit und Technischer Datenschutz“

Cybersicherheit

Cyberabwehr Bayern

Ransomware



Konfigurations-fehler

Zusammenarbeit national/ international

Was ist das für eine Behörde?

Bayerisches Landesamt für Datenschutzaufsicht (**BayLDA**)

- Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich in Bayern
- Aufgabe: Sicherstellung, dass sich alle bayerischen Unternehmen, Vereine, Rechtsanwälte, Ärzte, … an die DS-GVO halten
- Sitz in Ansbach
- 34 Planstellen für ca. 800.000 datenschutzrechtlich Verantwortliche
- Ist auch Bußgeldstelle nach DS-GVO

Was hat Datenschutz mit Cybersicherheit zu tun?

photonphoto@123rf.com

- Die DS-GVO definiert die Sicherheit personenbezogener anhand der Einhaltung der Vertraulichkeit, Verfügbarkeit und Integrität der Daten, der IT-Systeme und Fachprozesse
- Es müssen in Abhängigkeit des Risikos (für die Rechte und Freiheiten der von einer Verarbeitung betroffenen Personen) wirksame Schutzmaßnahmen gegen unbefugte Handlungen („Security“) und ungewollte Ereignisse („Safety“) getroffen werden
- Bedeutet: Kleine Vereine oder ein mittelständisches, produzierendes Gewerbe müssen (gar nicht teure) „Standardmaßnahmen“ umsetzen, Konzerne und datengetriebene Unternehmen i. d. R. deutlich höhere Schutzvorkehrungen
- Mängel in der Cybersicherheit sind bußgeldbewährt (10 Mio. Euro / 2 % Umsatz)

Cybersicherheit (bei personenbezogenen Daten) ist eine gesetzlich verpflichtende Anforderung in ganz Europa

Wieso sind Cyberattacken weiter so erfolgreich?

Quelle und Hintergrund: Herr der Ringe, Schlacht um Helms Klamm

Ausgangsbasis:

- Unternehmen schützen den Perimeter meist sehr gut
- Angreifer scheitern i. d. R. an der zentralen Firewall
- Auch Browser sind meist gut gepatcht

Wieso sind Cyberattacken weiter so erfolgreich?

Quelle und Hintergrund: Herr der Ringe, Schlacht um Helms Klamm - Ein Uruk-Krieger hat doch tatsächlich **die eine Schwachstelle** gefunden

Ausgangsbasis:

- Unternehmen schützen den Perimeter meist sehr gut
- Angreifer scheitern i.d.R. an der zentralen Firewall
- Auch Browser sind meist gut gepatcht

Wieso sind Cyberattacken weiter so erfolgreich?

Quelle und Hintergrund: Herr der Ringe, Schlacht um Helm
doch tatsächlich **die eine Schwachstel**

Bedeutung:

Das kleinste Einfallstor kann trotzdem die größte Wirkung entfalten und den Perimeter überwinden

Es geschieht täglich hundertfach

1 - Rahmenbedingungen:

- Alle Mitarbeiter haben regelmäßige Awareness-Schulungen
- IT-Sicherheit nach „Industriestandard“ wird im Unternehmen umgesetzt

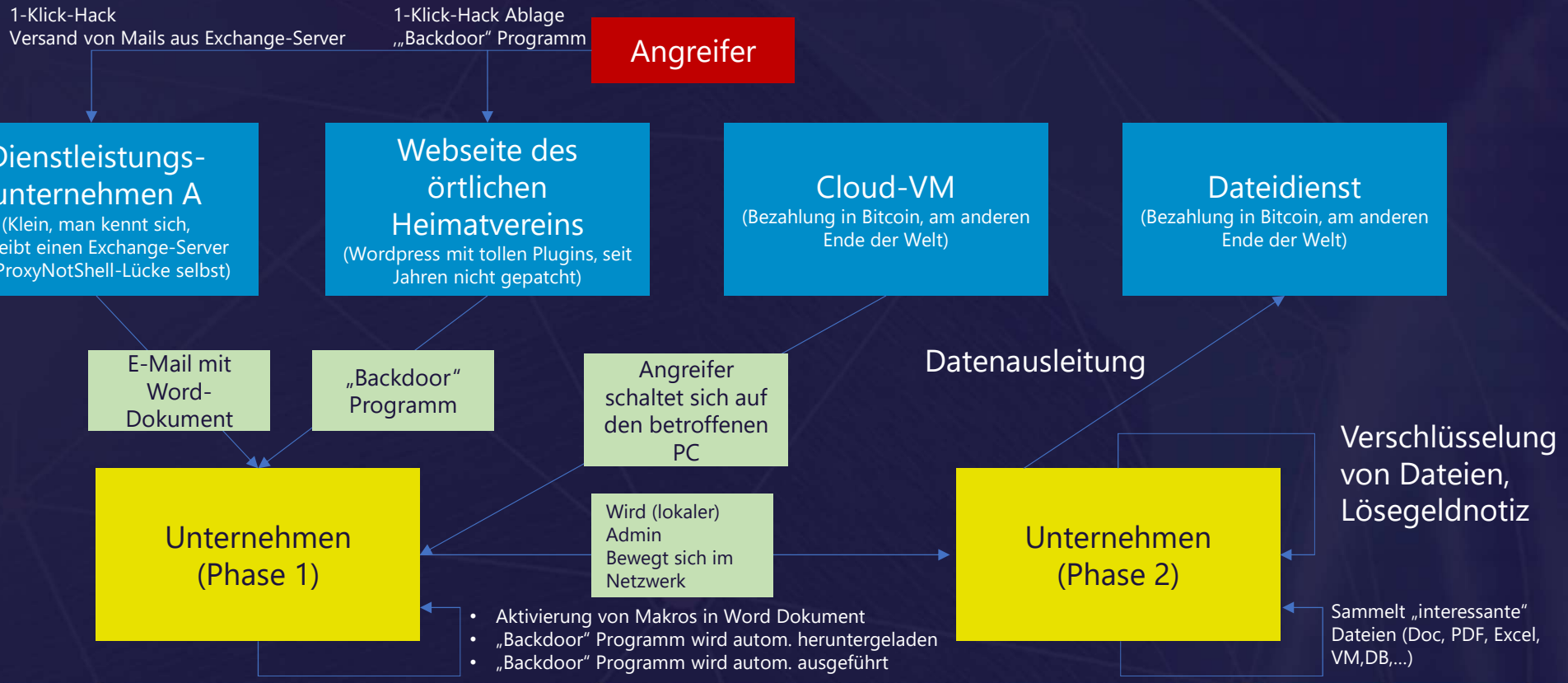
2 - Was passiert?

- E-Mail-Antwort eines bekannten Kommunikationspartners kommt
- Sprache und Kontext passen
- E-Mail-Absender ist echt, keine gefälschte E-Mail
- Einstufung des Mitarbeiters: Alles ok,
  Word-Dokument in Mail wird geöffnet und Makro aktiviert

3 - Bald darauf das Erwachen:

- Der zentrale Fileserver und alle virtuellen Maschinen sind verschlüsselt
- Es liegt eine Erpressernachricht vor, die als „Dienstleistung“ die Entschlüsselung samt „Sicherheitsberatung“ für nur 8 Mio. Euro anbietet

Details eines exemplarischen Angriffs



Incident Response bei betroffenen Unternehmen

Was tun im Notfall?

- Zuallererst bedeutet ein erfolgreicher Cyberangriff (wohl) das Worst-Case-Szenario für ein Unternehmen
- Neben der berechtigten Frage, wie das Unternehmen wieder betriebsbereit gebracht werden kann, müssen auch datenschutzrechtliche Meldepflichten innerhalb 72 Stunden eingehalten werden
- Meldung geht ganz unbürokratisch (z. B. unter www.lda.bayern.de/datenschutzverletzung)
- Auch sollte unbedingt Strafanzeige bei der Polizei gestellt werden
- Sofern ein Datenschutzbeauftragter bestellt ist: Diesen unbedingt in die Aufarbeitung einbinden
- Aus Datenschutzperspektive: Lösegeldzahlungen ändern nichts bei den Meldepflichten an betroffene Personen

Bayerisches Landesamt für
Datenschutzaufsicht

Incident Response bei betroffenen Unternehmen

Was tun im Notfall?

- Handeln Sie überlegt und schnell im Team
- Dokumentieren Sie Ihr Handeln
- Finden und Isolieren Sie den Infektionsherd
- Bestimmen Sie den Ransomware-Typ
- Bewerten Sie das Risiko für die betroffenen Personen
- Informieren Sie Ihre Mitarbeiterinnen und Mitarbeiter
- Vermeiden Sie die Kontaktaufnahme mit den Angreifern und die Zahlung von Lösegeld
- Starten Sie die Wiederherstellung der Daten

Defense in depth: Höhere Hürden für Angreifer

Acht wirksame Schutzmaßnahmen gegen Ransomware

01	Netzwerksegmentierung umsetzen	05	Administrative Passwörter variieren
02	PowerShell begrenzen	06	Internetübergang protokollieren und filtern
03	Programmausführung verhindern	07	Air-Gap-Backups einsetzen
04	Fremde Office-Makros unterbinden	08	Netzwerkkomponenten up-to-date halten

Denken Sie auch an die Auftragsverarbeitung

- DS-GVO adressiert Verantwortliche und Auftragsverarbeiter – letzte **Verantwortlichkeit** bleibt aber beim Auftraggeber
- Verantwortlicher muss sicherstellen, dass bei allen **Auftragsverarbeitern** und allen eingesetzten **Produkten**, die Anforderungen aus der DS-GVO erfüllt sind

Sicherheitslücke bei MOVEit:

- 2393 Organisationen
- 69 – 73,8 Millionen betroffene Personen

(Stand 16.11.2023)

Quelle: Enisa (2021)

Interesse an mehr Informationen?

- Cyberprävention:
  www.lda.bayern.de/de/cyberpraevention.html
- Ransomware-Prävention:
  www.lda.bayern.de/media/pruefungen/Ransomware_Praevention_Handreichung.pdf
- Checklisten:
  www.lda.bayern.de/de/checklisten.html

Vielen Dank für Ihre Aufmerksamkeit.

Cyberprävention
Mehr Sicherheit durch Datenschutz
www.lda.bayern.de