Bayerisches Landesamt für Datenschutzaufsicht

Cyberprävention

Mehr Sicherheit durch Datenschutz

Andreas Sachs

Vize-Präsident BayLDA
Bereichsleiter Cybersicherheit und technischer Datenschutz

Wer steht heute vor Ihnen?

Andreas Sachs

Bereichsleiter **Cybersicherheit und Technischer Datenschutz** &
Vize-Präsident beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA)

Technische Grundsatzfragen

Smart Things

Cybersicherheit

Automotive

Prüfstrategie Prüfverfahren

Verschlüsselung

Datenschutz-folgenabschätzung

Was ist denn das für eine Behörde?

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)

- Datenschutzaufsichtsbehörde für den sog. 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 (der Rechte und Freiheiten der von einer Verarbeitung betroffenen Personen) wirksame Schutzmaßnahmen gegen unbefugte Handlungen („Security“) und ungewollte Ereignisse („Safety“) getroffen werden
- Bedeutet: Kleine Heimatvereine 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 steht denn der Datenschutz mit dem Verfassungsschutz auf einer Bühne?

Bayerische Behörden mit Cybersicherheitsaufgaben

Bürger

Bayerische Unternehmen

Cyberabwehr Bayern

- Landesbeauftragter für den Datenschutz
- Zentralstelle Cybercrime Bayern
- Landesamt für Sicherheit in der Informationstechnik
- Landesamt für Verfassungsschutz
- Landeskriminalamt
- Landesamt für Datenschutzaufsicht

+ Cyber-Lagezentrum

„**Schild**“:
Kooperation und Information im Rahmen der gesetzlichen Möglichkeiten

Angreifer über das Internet

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 gepatched

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 gepatched

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 hundertfach auch in Bayern

1 - Rahmenbedingungen:

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

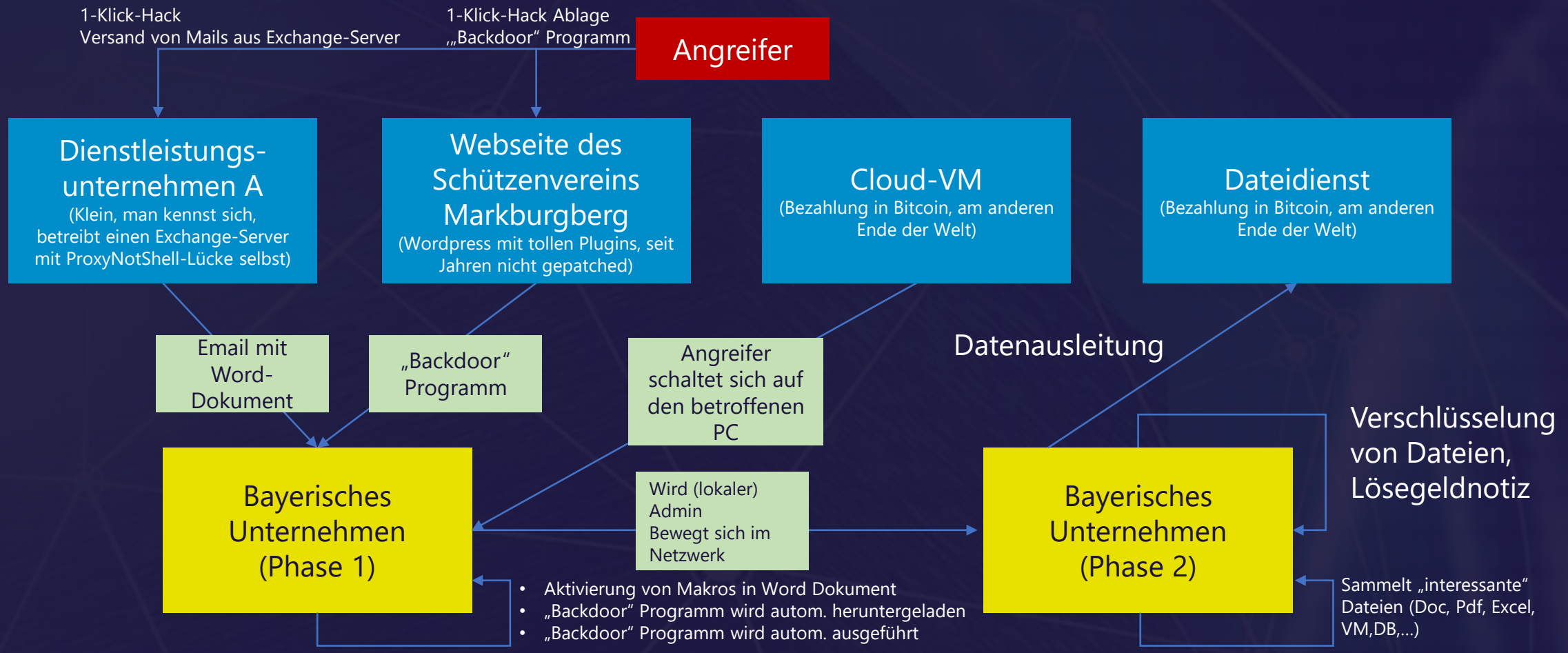
2 - Was passiert?

- 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 - Tags 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

Deep-Dive eines exemplarischen Angriffs

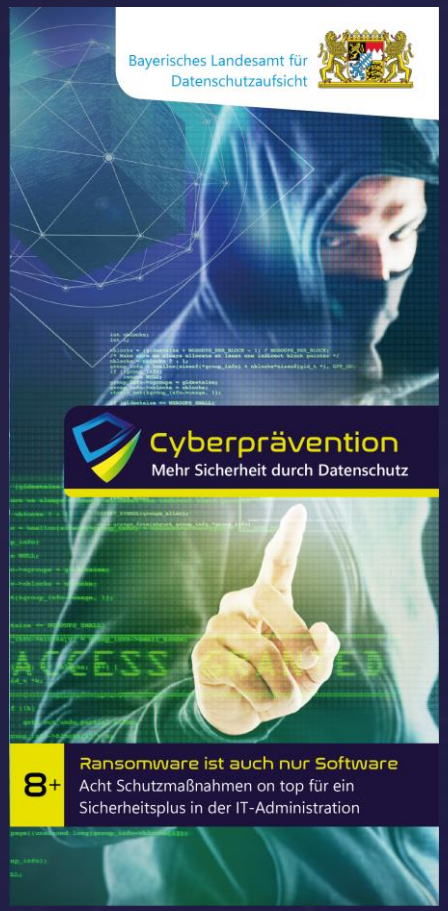


Incident Response bei betroffenen Unternehmen

Was tun im Notfall?

- Zu aller erst 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 unter www.lda.bayern.de/datenschutzverletzung
- Auch sollte unbedingt Strafanzeige bei der Polizei gestellt werden
- Aus Datenschutzperspektive: Lösegeldzahlungen ändern nichts bei den Meldepflichten an betroffene Personen
- Sofern ein Datenschutzbeauftragter bestellt ist: Diesen unbedingt in die Aufarbeitung einbinden

Defense in depth: Höhere Hürden für Angreifer



Acht wirksame Schutzmaßnahmen gegen Ransomware

gibt es zum Mitnehmen als Flyer an unserem Stand

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

Interesse an mehr Checklisten?

- Ransomware-Prävention:
  www.lda.bayern.de/media/pruefungen/Ransomware_Praevention_Handreichung.pdf
- E-Mail Account Abicherung:
  www.lda.bayern.de/media/pruefungen/Mail_Account_Praevention_Handreichung.pdf
- Cybersicherheit für medizinische Einrichtungen
  www.lda.bayern.de/media/checkliste/baylda_checkliste_medizin.pdf
- Patch Management
  www.lda.bayern.de/media/checkliste/baylda_checkliste_patch_mgmt.pdf
- Homeoffice
  www.lda.bayern.de/media/checkliste/baylda_checkliste_homeoffice.pdf
- Technische und organisatorische Datenschutz-Maßnahmen
  www.lda.bayern.de/media/checkliste/baylda_checkliste_tom.pdf

Mehr Informationen dazu an unserem Stand

Vielen Dank für Ihre Aufmerksamkeit.

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