Cyberprävention

Mehr Sicherheit durch Datenschutz

Bayerisches Landesamt für Datenschutzaufsicht

Ransomware Prävention

für kleine und mittlere Unternehmen

Andreas Sachs

Vize-Präsident BayLDA

Bereichsleiter Cybersicherheit und technischer Datenschutz

nada01@123rf.com, peopleimages12@123rf.com

Wer sitzt heute (virtuell) 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 Ransomware zu tun?

photonphoto@123rf.com

- Die DS-GVO definiert die Sicherheit personenbezogener Daten 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
- Ransomware ist weiterhin Top 1 Risiko im Bereich internetbasierte Kriminalität gegen Unternehmen
- Datenschutzrisiko (Fokus auf Betroffene Personen): Primär Datenausleitung
- Unternehmensrisiko (Fokus auf Betriebe): Primär Verfügbarkeitsstörung Geschäftsprozesse und Reputationsschäden

→ **Ransomware-Prävention (bei personenbezogenen Daten) ist eine gesetzlich verpflichtende Anforderung in ganz Europa**

→ **Synergien zwischen Datenschutz und (Unternehmens)-IT-Sicherheit können hier hervorragend genutzt werden**

Wieso sind Cyberattacken weiter so erfolgreich?

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

Ausgangsbasis:

- (Auch kleinere) Unternehmen schützen den Perimeter meist sehr gut
- Angreifer scheitern i.d.R. an der zentralen Firewall
- Auch Browser sind meist gut (automatisch) gepatched

Wieso sind Cyberattacken weiter so erfolgreich?

ABER!

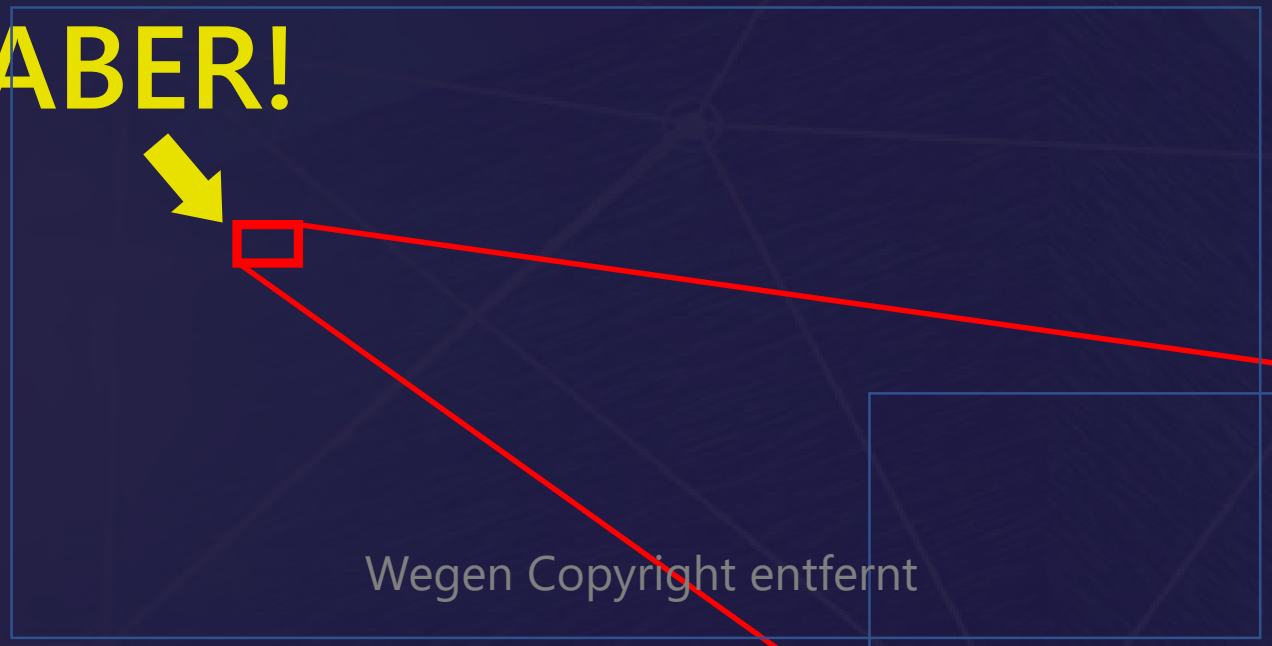
Quelle und Hintergrund: Herr der Ringe, Schlacht um Helms Klamm - Ein Uruk-Krieger hat doch tatsächlich **die eine Schwachstelle** gefunden

Ausgangsbasis:

- (Auch kleinere) Unternehmen schützen den Perimeter meist sehr gut
- Angreifer scheitern i.d.R. an der zentralen Firewall
- Auch Browser sind meist gut (automatisch) gepatched

Wieso sind Cyberattacken weiter so erfolgreich?

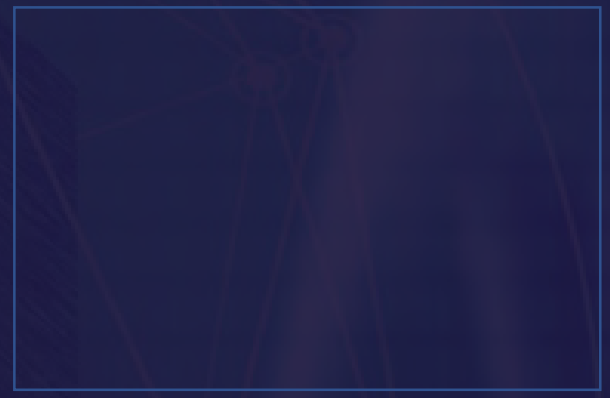
ABER!



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

Bedeutung:

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



Es geschieht tausendfach in ganz Deutschland

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 (Chat-GPT macht es noch leichter)
- 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

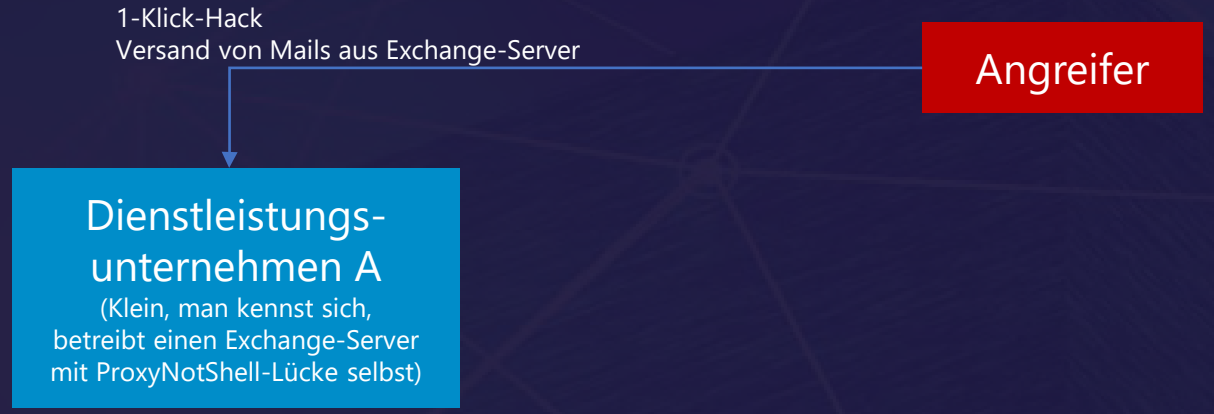
studiostoks@123rf.com

Deep-Dive eines exemplarischen Angriffs

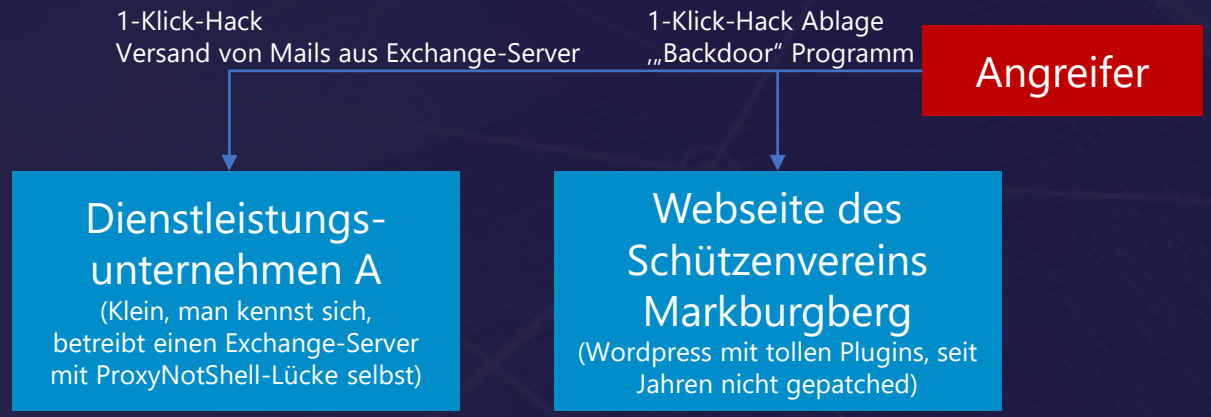
- Ein Hacking-Angriff ist keine Zauberei
- Aber meist schon ziemlich gute „Handwerkskunst“
- Ransomware-Gruppierungen agieren wie Wirtschaftsunternehmen:
  - Man kann sich „bewerben“ – wenn man Angriffe auf Niveau von guten Pentestern nachweisen kann
  - Es gibt teilweise eine Art „Affiliate“-System
  - Es gibt eine Sammlung von Softwaretools und Anleitungen
  - Es gibt eine Infrastruktur zur „Kundenkommunikation“
  - Auch das Verschlüsseln von Daten kann mit 1-Klick durchgeführt werden
  - Es gibt eine hohe Dynamik an Gruppierungen, „Angestellten“ und Angriffsmethoden
- Schauen wir uns die einzelnen Schritte nun mal an …
- … und überlegen uns dann, wie man sich davor schützen kann.

studiostoks@123rf.com

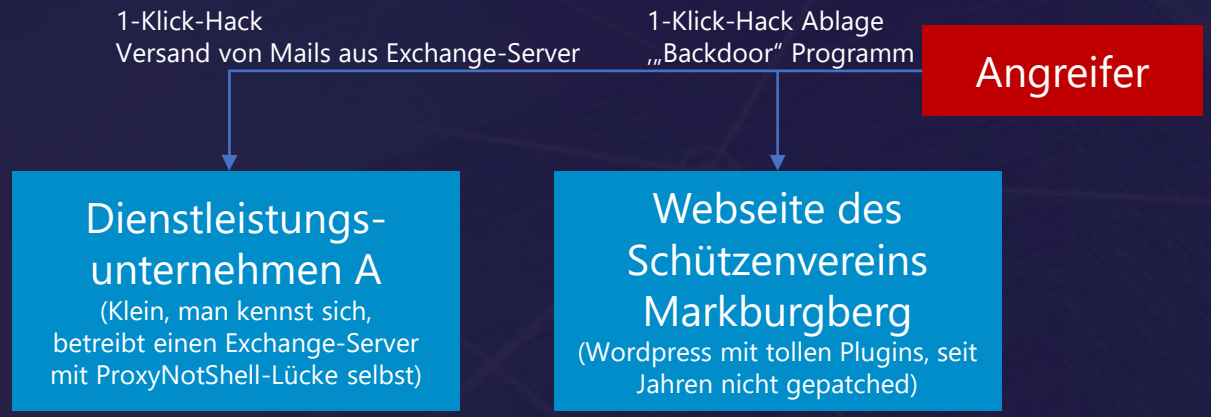
Deep-Dive eines exemplarischen Angriffs



Deep-Dive eines exemplarischen Angriffs

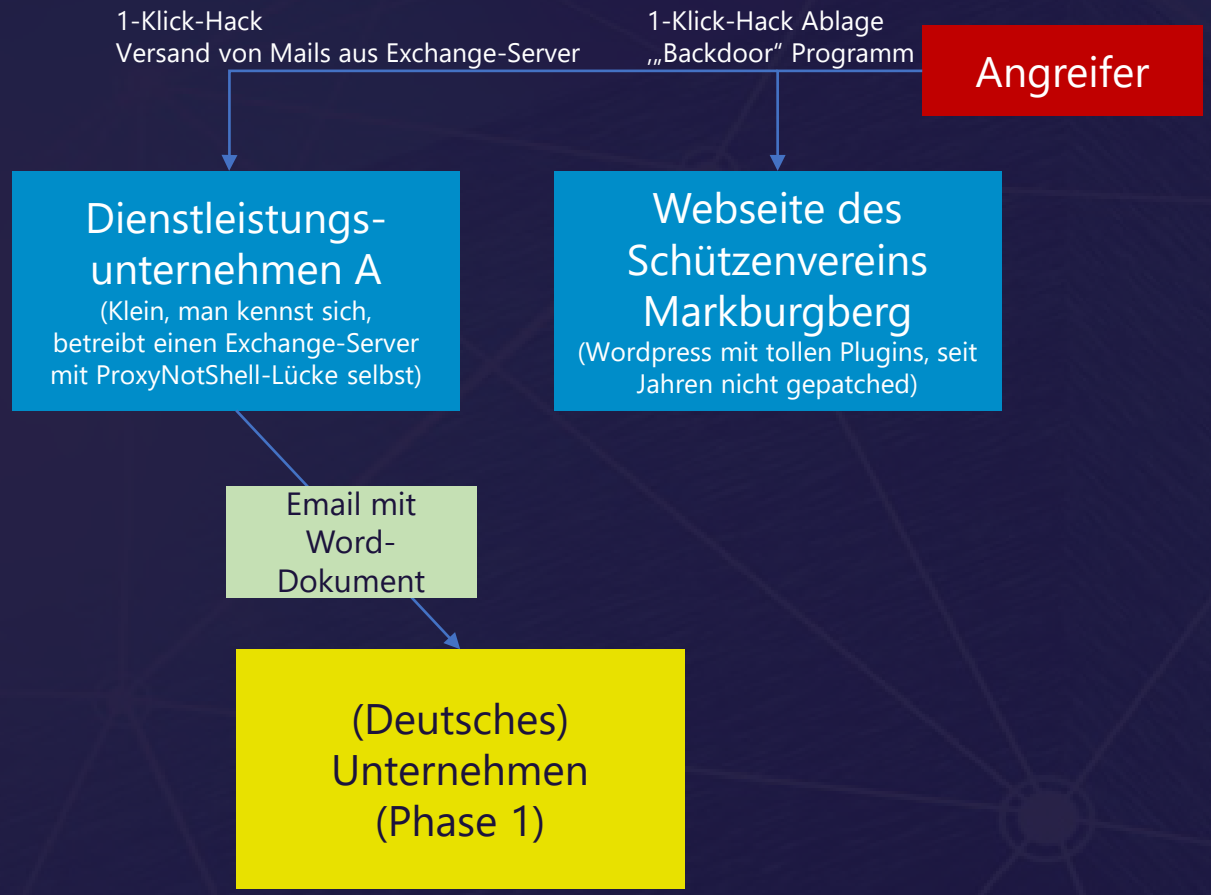


Deep-Dive eines exemplarischen Angriffs

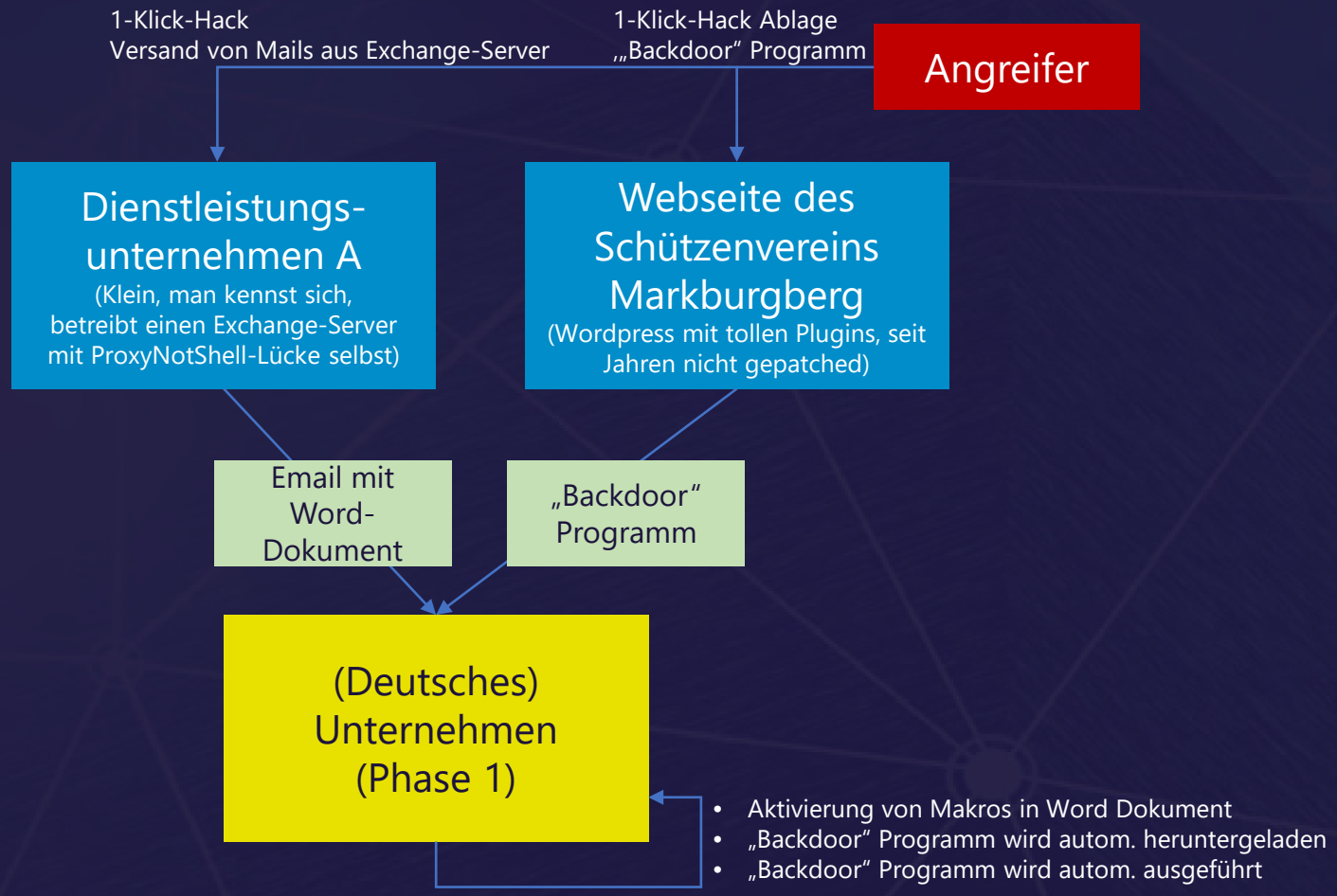


(Deutsches) Unternehmen

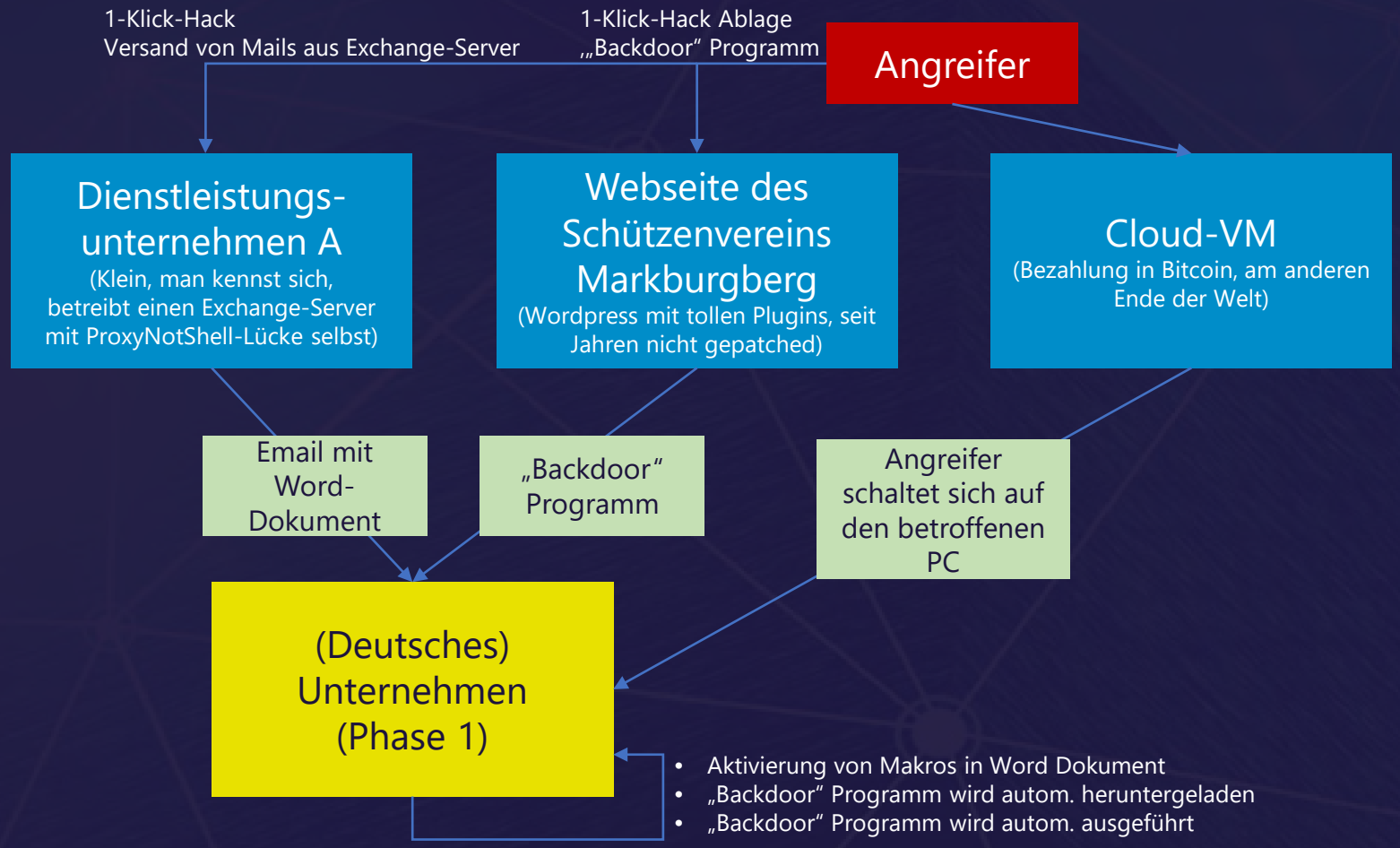
Deep-Dive eines exemplarischen Angriffs



Deep-Dive eines exemplarischen Angriffs



Deep-Dive eines exemplarischen Angriffs



Wo stehen wir?

Unternehmensnetzwerk

Angreifer

- Angreifer ist im Unternehmensnetzwerk
- Hat eine Kommandozeile mit Rechten der Person, die das Word-Dokument geöffnet hat
- Im Prinzip wie ein sog. Innentäter
- Nur hat dieser Pentest-KnowHow und Software-Tools für weitere Angriffe

Wo stehen wir?

Unternehmensnetzwerk

Angreifer

- Angreifer ist im Unternehmensnetzwerk
- Hat eine Kommandozeile mit Rechten der Person, die das Word-Dokument geöffnet hat
- Zum Beispiel Sekretärin, Vertrieb, Entwicklung, Einkauf, Personal,…
- Im Prinzip wie ein sog. Innentäter (bislang) ohne privilegierte Benutzerrechte
- Nur hat dieser Pentest-KnowHow und Angriffs-Software-Tools

Hier schon mal die erste Security Maßnahme

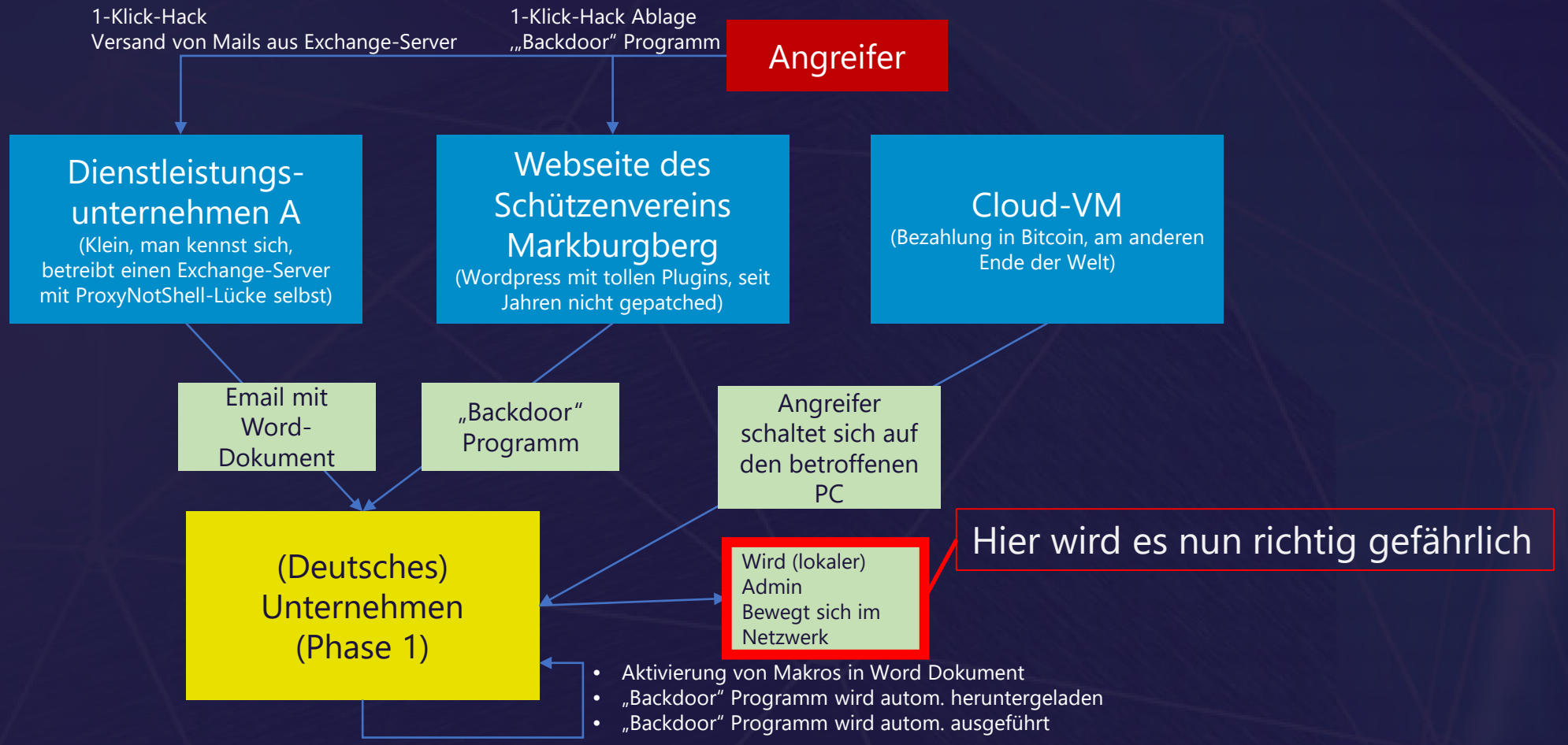
Standard Security-Maßnahme

Niemals mit Administrationsrechten andere Tätigkeiten ausführen wie Mails bearbeiten oder im Internet surfen

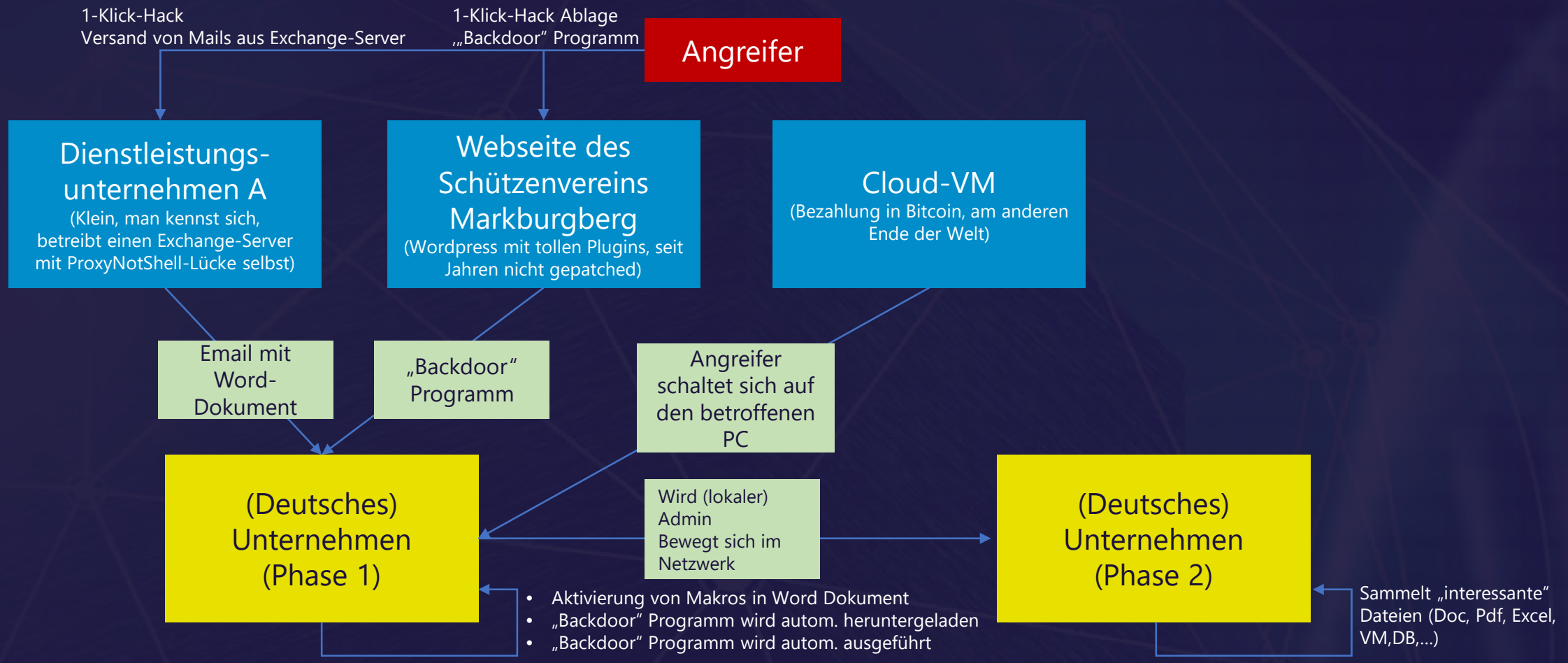
Falls nämlich doch:
Angreifer ist (Domänen)-Admin

makstorm@123rf.com

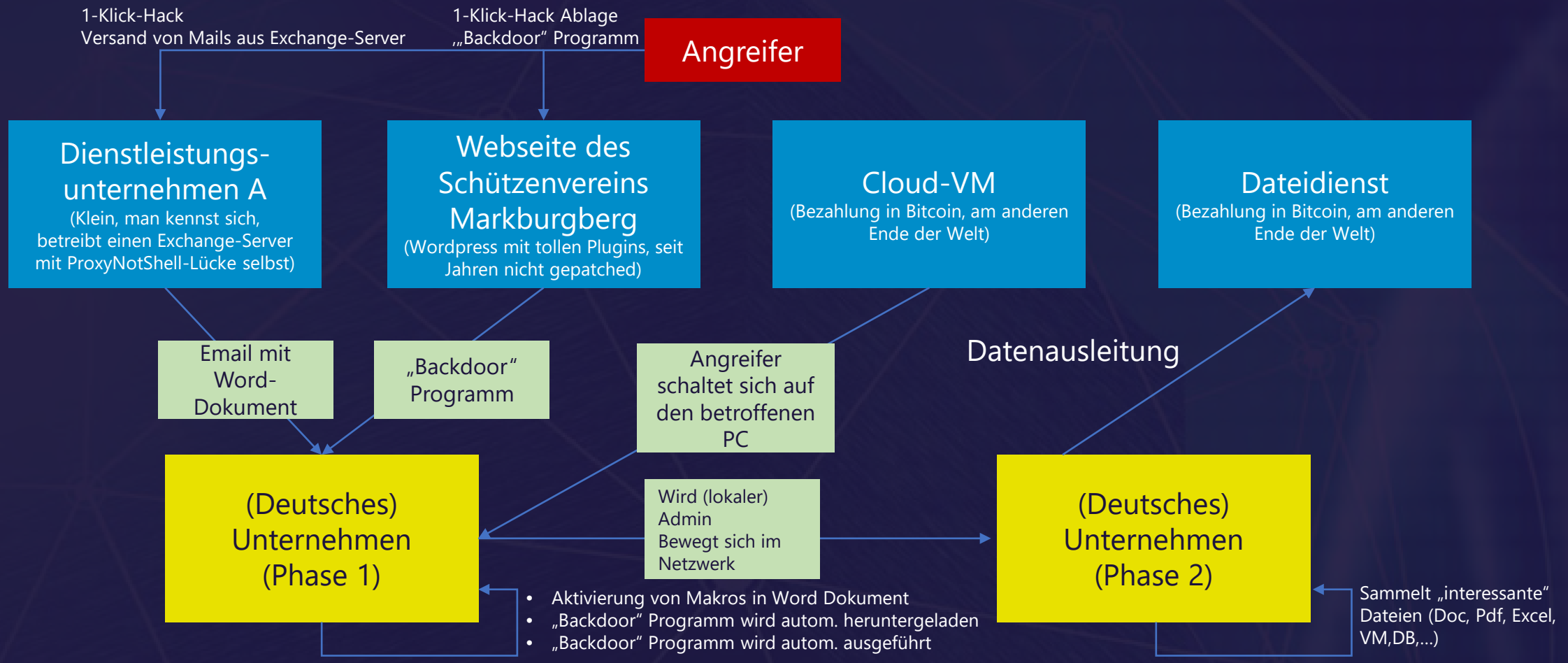
Deep-Dive eines exemplarischen Angriffs



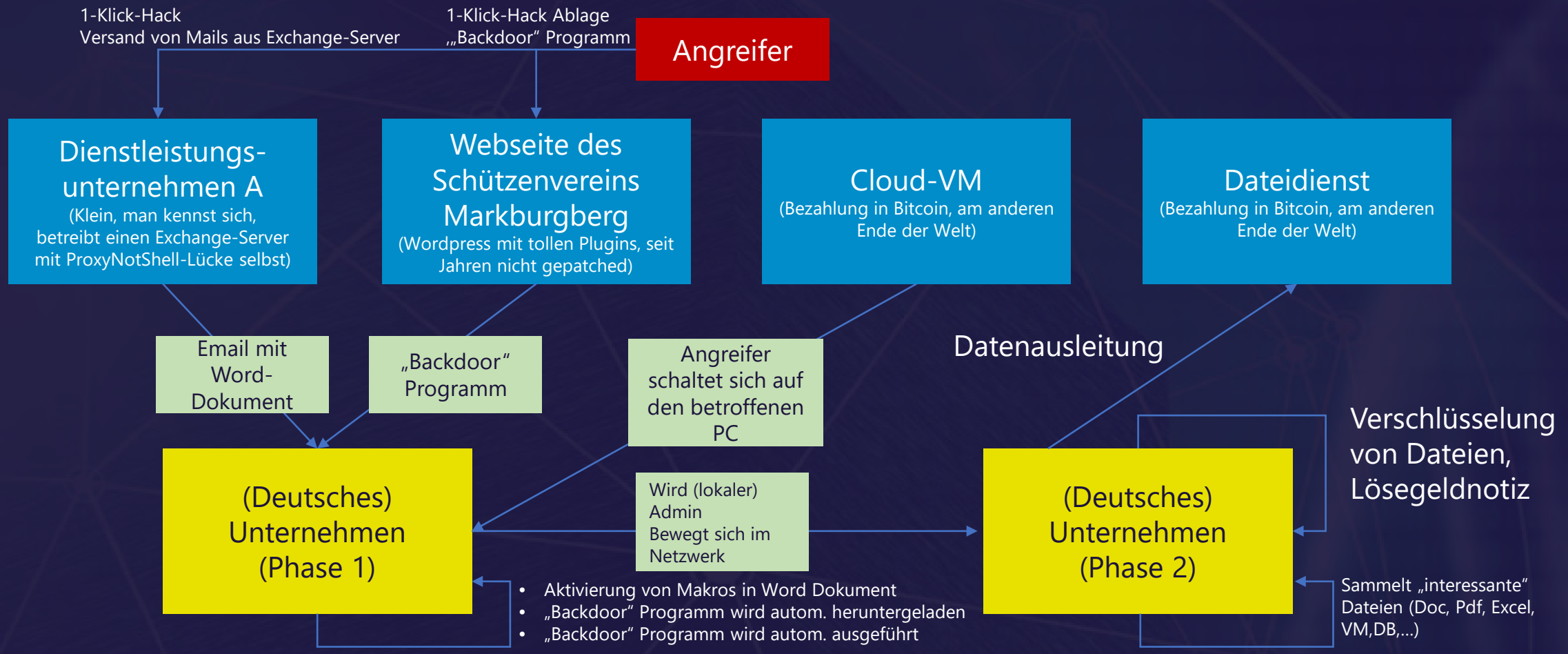
Deep-Dive eines exemplarischen Angriffs



Deep-Dive eines exemplarischen Angriffs



Deep-Dive eines exemplarischen Angriffs



Deep-Dive eines exemplarischen Angriffs

1-Klick-Hack
Versand von Mails aus Exchange-Server

1-Kl
„Ba

Dienstleistungs-
unternehmen A
(Klein, man kennst sich,
betreibt einen Exchange-Server
mit ProxyNotShell-Lücke selbst)

W
Sch
Ma
(Wordpre
Jahr

Dateidienst
(Bezahlung in Bitcoin, am anderen
Ende der Welt)

Email mit
Word-
Dokument

„Backdo
Progra

eitung

(Deutsches)
Unternehmen
(Phase 1)

eutsches)
ternehmen
Phase 2)

Verschlüsselung
von Dateien,
Lösegeldnotiz

Sammelt „interessante“
Dateien (Doc, Pdf, Excel,
VM,DB,...)

- „Backdoor“ Programm wird autom. ausgeführt

Incident Response bei betroffenen Unternehmen

Was tun im Notfall?

- Zu aller erst bedeutet ein erfolgreicher Cyberangriff (wohl) das Worst-Case-Szenario für ein Unternehmen
- Falls funktionierende Backups vorhanden sind, ist immer noch die Datenausleitung kritisch
- Neben der berechtigten Frage, wie das Unternehmen wieder betriebs-bereit gebracht werden kann, müssen auch datenschutzrechtliche Meldepflichten innerhalb 72 Stunden eingehalten werden
- Meldung in Bayern 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
- Aus Unternehmensperspektive: Lösegeldzahlung mitunter die Alternative zum Konkurs.
- Gedankenspiel: Wir würde ihr Unternehmen funktionieren, wenn alle

Incident Response bei betroffenen Unternehmen

Was

Gedankenspiel:
Wie wäre es für Sie und ihr Unternehmen, wenn alle internen Server und Datenbanken heute Nachmittag „weg“ wären und Angreifer dazu mit der Veröffentlichung von Patenten, Verträgen und allen Mitarbeiterdaten drohen?

Und Sie dann noch feststellen, dass die Backups auch gelöscht wurden!

Was tun? Es gibt bei Ransomware an sich nur 2 Möglichkeiten

Quelle: zeit.de

Repression

learchitecto@123rf.com

Prävention

IT-Sicherheit ist eine Datenschutzanforderung

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)
Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)

Cybersicherheit für medizinische Einrichtungen

Checkliste mit Prüfkriterien nach Art. 32 DS-GVO

Stand: 22. Juli 2020

Ziel und Inhalt dieses Papiers

Diese Handreichung ermöglicht einen Überblick einiger Praxismaßnahmen zur Cybersicherheit für medizinische Einrichtungen – inklusive eines Themenblocks speziell für Labore – entsprechend den geltenden gesetzlichen Datenschutzvorgaben. Im Sinne einer gezielten Prävention soll damit eine gesteigerte Sensibilisierung für sicherheitsrelevante Themen erreicht und aktiv ein störungsfreier Betrieb dieser Einrichtungen unterstützt werden. Der Fokus des Dokuments liegt auf der Verfügbarkeit der Daten bzw. Dienste bezüglich Angriffe aus dem Internet und weniger auf deren Vertraulichkeit und Integrität, die aus Datenschutzsicht jedoch ebenfalls zu beachten sind. Die aufgeführten Maßnahmen sind selbstverständlich nicht als abschließend zu betrachten, sondern stellen eines Best-Practice-Ansatz dar, der einen effektiven Schutz gegen aktuelle Cybersicherheitsbedrohungen unterstützen kann. Auf Grund der individuellen Gegebenheiten jedes Betriebs ist es nicht zwingend erforderlich, jede genannte Maßnahme zur Einhaltung der datenschutzrechtlichen Sicherheitsanforderungen umzusetzen. Werden einzelne Maßnahmen nicht umgesetzt, ist zu prüfen, wie andere (ggf. bestehende) Maßnahmen ein vergleichbares angemessenes Schutzniveau bieten können.

Bei diesem Papier handelt sich um eine Hilfestellung zur schnellen Überprüfung der eigenen Sicherheit hinsichtlich der Verfügbarkeit der eigenen Datenverarbeitung im Sinne von Art. 32 DS-GVO. Der Anwendungsbereich umfasst sowohl den nicht-öffentlichen als auch den öffentlichen Bereich. Das Werk entstand in einer Zusammenarbeit des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) und des Bayerischen Landesbeauftragten für den Datenschutz (BayLfD). Weiterführende Links zu vertrauenswürdigen Websites helfen bei der eigenen Umsetzung. Bei Fragen stehen das BayLDA und der BayLfD bereitend zur Seite.

Selbst-Check: Cybersicherheit in medizinischen Einrichtungen

1 Patch Management

Veraltete Softwarestände bergen ein erhöhtes Angriffsrisiko wegen potentieller Schwachstellen. Die eingesetzte Software muss daher durch regelmäßige Sicherheitsupdates aktuell gehalten werden.

- Konzept zum Patch Management vorhanden (u. a. Update-Plan mit Übersicht der eingesetzten Software)
- Regelmäßige Auswertung von Informationen zu Sicherheitslücken der eingesetzten Software wie Betriebssysteme, Office-Software, Fachanwendungen und medizinische Gerätesteuerung (z. B. durch E-Mail-Newsletter, Herstellerveröffentlichungen, Fachmedien, Sicherheitswarnungen)
- Ausschließlicher Einsatz von Desktop-Betriebssystemen, für die der Hersteller/Anbieter beim Bekanntwerden von Schwachstellen Sicherheitsupdates zur Verfügung stellt
- Geregelter Prozess zum zeitnahen Einspielen von Sicherheitsupdates der Server
- Automatische Updates der Desktop-Betriebssysteme (direkt vom Hersteller oder durch zentrale Verteilung)
- Geregelter Prozess für Updates von Basiskomponenten wie z. B. Java, PDF-Reader (Empfehlung: Automatisch, sofern möglich)

→ Weitere Informationen:
www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/OPS/OPS_1_1_3_Patch-_(BSI)

2 Malware-Schutz

Ein Befall mit Schadcode führt oft zu einer erheblichen IT-Störung. Durch Antiviren-Programme werden zwar nicht alle Schadcode-Varianten erkannt, aber viele Standardangriffe abgefangen. Ein wirksamer Anti-Malware-Schutz ist folglich einzusetzen.

- Endpoint Protection auf jedem Arbeitsplatzrechner
- Tägliche automatische Aktualisierung der Antivirensignaturen
- Zentrale Erfassung von Alarmmeldungen durch die IT-Administration
- Klare Anweisungen an Beschäftigte zum Umgang mit Alarmmeldungen
- Ablaufplan der IT-Administration bei Malware-Befall
- Antivirenlösung mit als „hoch" konfigurierter lokaler heuristischer Erkennung
- Sandboxing-Verfahren oder Advanced Endpoint Protection und Response (EDR) nur unter strenger Berücksichtigung datenschutzrechtlicher Vorschriften

→ Weitere Informationen:
www.lda.bayern.de/de/thema_schadcode.html (LDA)

Bayerisches Landesamt für Datenschutzaufsicht

Datenschutzrechtliche Regelungen bei Homeoffice

Checkliste mit Prüfkriterien nach DS-GVO

Stand: 25. Juni 2021

Ziel und Inhalt dieses Papiers

Die Corona-Pandemie hat viele Unternehmen, Selbstständige und Freiberufler mit der Frage konfrontiert, wie die Arbeitsfähigkeit weiterhin sichergestellt und zeitgleich Maßnahmen zur Eindämmung des infektionsgeschehens getroffen werden können. Bei bestimmten Tätigkeiten führte dies dazu, dass das Arbeiten von zu Hause aus sehr schnell erwertet oder neu eingeführt wurde. Diese Handreichung soll hierfür einen Überblick über die wichtigsten Praxismaßnahmen im Homeoffice entsprechend den geltenden gesetzlichen Datenschutzvorgaben geben. Im Sinne einer gezielten Prävention von Datenschutzverstößen soll damit im „neuen Alltag" eine gesteigerte Sensibilisierung für dieses Thema erreicht und mit konkreten Prüfpfragen der eigene Stand der Umsetzung unterstützt werden. Die aufgeführten Prüfpunkte sind nicht als abschließend zu betrachten, sondern stellen einen Best-Practice-Ansatz dar, der bspw. von Seiten der Geschäftsführung oder des Datenschutzbeauftragten im Sinne einer Soll-Ist-Übergrüfung verwendet werden kann. Dabei ist es nicht immer bei allen Punkten der Fall, dass diese umgesetzt zwangsläufig werden müssen – dann ist jedoch eine kritische Hinterfragung des Grundes samt kurzer Dokumentation angeraten.

Selbst-Check: Datenschutzrechtliche Regelungen bei Homeoffice

1 Arbeitsumgebung

Die Arbeitsplatzumgebung zu Hause soll so ausgestaltet sein, dass vom Grundsatz her die Vertraulichkeit und Verfügbarkeit der Daten wie im Büro sichergestellt ist.

- Der Arbeitsplatz ist so gewählt, dass Familienmitglieder oder Besucher keinen Blick auf das Notebook und in die Papierunterlagen werfen können
- Es gilt eine Clean-Desk-Policy am Ende des Arbeitstages.
- Es werden Sichtschutzfolien angebotet, wenn dies erforderlich ist (bspw. Schreibtisch am Fenster in Parterrewohnung)
- Papierunterlagen können in Dokumentenmappen oder Schränken verschlossen werden.
- Fenster werden in Erdgeschosswohnungen bei Verlassen des Arbeitsplatzes immer geschlossen.
- Sperrung des Notebooks bei Verlassen des Arbeitsplatzes, falls ein anderer Zugriff – egal ob gewollt oder ungewollt z. B. durch Kinder oder Haustiere – nicht ausgeschlossen ist
- Es wird darauf geachtet, dass Telefongespräche nicht von unbefugten Personen mitgehört werden (z. B. offenes Fenster, laufende andere Videokonferenz)

2 Genutzte Hardware

Es wird der Bereitstellung von dienstlichen Geräten empfohlen. Privatgeräte sollten nur in Ausnahmefällen eingesetzt werden.

- Dienstliche Notebooks werden gestellt
- Dienstliche Smartphones oder Softphones werden gestellt
- Bei Verwendung von Privatgeräten werden Restriktionsverfügungen auf Terminalserver verwendet
- Dienstlich zur Verfügung gestellte Geräte werden auch zu Hause nicht für private Zwecke genutzt

3 Umgang mit Papierdokumenten

In vielen Betrieben sind noch nicht alle Arbeitsabläufe komplett digital nutzbar. Beim Umgang mit Papierdokumenten entstehen neue Risiken, die in den Räumlichkeiten des Büros nicht auftraten.

- Papierunterlagen werden in geeigneten Mappen (u. a. mit Name des Unternehmens im Falle eines Verlusts) mit nach Hause genommen
- Regelungen bestehen, dass Papierunterlagen beim Transport nach/von zu Hause nicht erhöhten Risikosituationen (z. B. Rücklotz beim Einkaufen, Rucksack im Restaurant) ausgesetzt werden sollen.
- Entsorgung von Papierunterlagen erfolgt nicht über den eigenen Hausmüll, sondern fachgerecht entweder im Büro oder zu Hause durch einen Aktenvernichter mit mind. Sicherheitsstufe 3 nach DIN 66399)
- Es wurde über die Risiken der Schädigung von wichtigen Papierdokumenten (z. B. Kinder bemalen ein Originaldokument) sensibilisiert – es wird bei solchen Dokumenten, sofern möglich, mit Kopien gearbeitet

4 Nutzung von Videokonferenzsystemen

Bei der Auswahl von Videokonferenzlösungen, mit denen Präsenzbesprechungen teilweise oder vollständig ersetzt werden, müssen bestimmte Anforderungen beachtet werden.

- Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO ist abgeschlossen
- Bei Anbietern in unsicheren Drittländern sind geeignete Garantien vorhanden, es wird dabei insbesondere geprüft, ob bei Nutzung von Standarddatenschutzklauseln zusätzliche Schutzmaßnahmen im Sinne des Schrems II Urteils erforderlich sind

Bayerisches Landesamt für Datenschutzaufsicht

Patch Management im Alltag

Checkliste nach Art. 32 DS-GVO

Stand: 22. Juli 2020

Ziel und Inhalt dieses Papiers

Die vorliegende Handreichung unterstützt vor allem kleine und mittlere Unternehmen dabei, festzustellen, wo und wie ein bedarfsgerechtes Aktualisieren der eingesetzten Softwaresysteme durchzuführen ist. Auch für Freiberufler, Selbstständige und andere Verantwortliche können einige Prüfpunkte dieser Checkliste von Nutzen sein. Das Risiko von Cyberattacken kann bereits durch regelmäßige Sicherheitsupdates erheblich reduziert werden, wenn vorhandene Schwachstellen erfolgreich geschlossen werden. Patch Management beschäftigt sich insbesondere mit dem Beschaffen, dem Testen und dem Einspielen wichtiger Updates für Anwendungen. Patches sind als Korrekturen zu betrachten, um gesetzt bekannte Fehler und Schwachstellen zu beheben, die ansonsten den sicheren Betrieb gefährden. Aus datenschutzrechtlicher Sicht besteht nach Art. 32 DS-GVO eine gesetzliche Anforderung, personenbezogene Daten angemessen zu schützen. Verantwortliche müssen demnach Verfahren etablieren, um regelmäßig überprüfen, bewerten und evaluieren zu können, ob die eigenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung auch tatsächlich wirksam sind. Patch Management spielt folglich eine zentrale Rolle im Sicherheitsumfeld und im Datenschutz. Maßnahmen aus dieser Handreichung zeigen, wie Patch Management in verschiedenen Bereichen einfach gelingen kann. Die aufgeführten Kriterien stellen einen Best-Practice-Ansatz dar und sollen in erster Linie als Einstieg für die wesentlichen Fachbereiche dienen.

Selbst-Check: Patch Management

1 Grundlagen

Das Installieren von Updates stellt zwar den wichtigsten Schritt beim Patch Management dar, bedarf aber noch Unterstützung. Vorhandene Patches müssen bekannt sein, zeitnah beschafft und auf den eigenen Systemen getestet sowie dokumentiert werden.

- Planen:
  Ein Plan zum Patch Management ist vorhanden (z. B. Welche Hard- und Software wird eingesetzt? Wer ist wofür zuständig? Welche Prozesse müssen beachtet werden?)
- Beschaffen:
  Informationen zu Updates werden gezielt gesucht bzw. Sicherheitshinweise einst genommen; nur seriöse Quellen werden als Patch-Source genutzt
- Testen:
  Patches für kritische Anwendungen werden nicht ungetestet in der Produktionsumgebung installiert, sondern erst nach ausreichender Prüfung eingespielt (Testumgebung), nach dem Patch wird der IT-Betrieb auf Funktionalität geprüft
- Installieren:
  Das Einspielen von Updates erfolgt kontrolliert, um unnötige Ausfallzeiten im alltäglichen Betrieb zu vermeiden
- Dokumentieren:
  Änderungen am System bleiben nachvollziehbar und können so jederzeit nachvollzogen und ggf. nachjustiert werden

→ Weitere Informationen:
www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/OPS/OPS_1_1_3_Patch-_(BSI)

2 Organisation

Patch Management ist keine Disziplin, die isoliert von anderen Fachbereichen der Organisation behandelt werden kann, da sie sich über alle Systeme und Dienste erstreckt. Eine angemessen Verankerung in den eigenen Organisationsstrukturen ist daher wichtig, um Patches nicht nur rechtzeitig und richtig einzuspielen, sondern auch negative Auswirkungen auf den Betrieb zu vermeiden.

- Patch Management ist fester Bestandteil der IT-Organisation
- Eigene Zuständigkeiten und Verantwortlichkeiten in der IT-Organisation sind definiert und kommuniziert (z. B. Wer patcht was? Wer kümmert sich um die Recherche von Schwachstellen?)

Bayerisches Landesamt für Datenschutzaufsicht

Selbst-Check: Sicherheit der Verarbeitung nach Art. 32 DS-GVO

1 Management und Organisation

Mangelhafte Sicherheitsstrukturen in einer Organisation können den Betriebsablauf erheblich gefährden. Bestehende Fachkompetenzen sind daher zu nutzen. Dabei ist nicht nur der IT-Verantwortliche, sondern auch der Datenschutzbeauftragte (DSB) im Prozess der Umsetzung von Sicherheitsanforderungen einzubinden.

- Eine geeignete Organisationsstruktur für Informationssicherheit ist vorhanden und die Informationssicherheit ist in die organisationsweiten Prozesse und Abläufe integriert
- Sicherheitsrichtl- und -leitlinien sind definiert, von der Geschäftsleitung genehmigt und dem Personal kommuniziert
- Die Rollen der einzelnen Mitarbeiter im Sicherheitsprozess sind eindeutig festgelegt
- Regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen nach dem PDCA-Zyklus (Plan-Do-Check-Act)
- Konzepte und Dokumentationen im Sicherheitsumfeld werden regelmäßig überprüft und aktuell gehalten.
- Je nach Unternehmensgröße Einsatz eines geeigneten Informationssicherheitsmanagementsystem (ISMS), z. B. nach ISO/IEC 27001, BSI Standards oder IS/12
- Die Rollen und Verantwortlichkeiten im Bereich der Sicherheit sind im eigenen Betrieb bekannt und besetzt (u. a. Informationssicherheitsbeauftragter (ISB), IT-Leiter, Datenschutzbeauftragter (DSB))
- Konsequente Einbindung des DSB bei Sicherheitsfragen
- Ausreichende fachliche Qualifikation des DSB für sicherheitsrelevante Fragestellungen und Möglichkeiten zur Fortbildung für dieses Thema.
- Durchführung von regelmäßigen Audits des DSB nach Art. 32 DS-GVO zur Sicherheit der Verarbeitung
- Kenntnis der zuständigen Datenschutzaufsichtsbehörde sowie Wissen über die Meldeverpflichtungen nach Art. 33 und 34 DS-GVO (Verletzung der Sicherheit)
- Vorhandensein von Eskalationsprozessen bei Sicherheitsverletzungen (Wer ist wann wie zu informieren?), u. a. im Notfallmanagement
- Konsequente Dokumentation bei Sicherheitsvorkommnissen (Security Reporting)
- Aktive Unterstützung der Zusammenarbeit des DSB mit dem ISB durch die Unternehmensleitung
- Erkenntnisse über (neue) digitale Bedrohungen sind zu sammeln und potentielle Auswirkungen auf den eigenen Betrieb abzuleiten

2 Physikalische Sicherheit der Infrastruktur

Der persönliche Zugang zu IT-Systemen und personenbezogenen Daten muss Unbefugten erschwert werden. Ebenso sind gravierende Schäden durch (Natur-)Ereignisse wie Feuer oder Wasser bestmöglich zu verhindern.

- Es besteht ein umfassendes Gesamtkonzept zur Gebäudesicherung im Allgemeinen (z. B. Brandschutz, Zutrittsbeschränkung und -kontrolle)
- Es besteht ein Konzept zu Zutrittsregelungen und zur physischen Zugangskontrolle (Perimeterschutz)
- Klare Regelungen zum Umgang mit Besuchern (z. B. Begleitung, Sicherheitszonen, Besucherausweise, Protokollierung, Zuständiger Mitarbeiter für Besucher) als Bestandteil des Konzepts
- Gelebte Regelungen zum Umgang auch mit externen Dienstleistern (z. B. bei Werkverträge, Handwerker, Wartung von Systemen) – wie Verschwiegenheitserklärung, persönliche Begleitung in Sicherheitszonen oder Protokollierung
- Schaffung von verschiedenen Sicherheitszonen (z. B. Besucherbereich, Serverräume, Arbeitsplätze, Forschungsbereich)
- Bei Sicherheitszonen: Aktuelle Übersicht zur Berechtigungsverwaltung (Welcher Mitarbeiter darf in welche Zone?)
- Bei Sicherheitszonen: Zugang zu Sicherheitszonen mit geeigneter Technik begrenzen (über Schlüssels/Chipkarten, ggf. auch weiteren Faktoren)
- Bei Sicherheitszonen: Bei Zonenübergang selbstschließende Türen einsetzen
- Bei Sicherheitszonen: Ggf. Beschilderung, welche Zone nicht betreten werden sollte/darf
- Sichere Schließsysteme samt dokumentierter Schlüsselverwaltung
- Es besteht ein Konzept zum Brandschutzkonzept
- Verwendung von Feuer-/Rauchmeldeanlagen (im Rahmen des Brandschutzkonzepts)
- Einsatz von automatischen Löschsystemen in Serverräumen (z. B. CO_2-Löschung) unter Berücksichtigung von Arbeitsschutzvorschriften
- Feuerhemmende Schränke/Tresore zur Lagerung essentieller Komponenten (z. B. Backup-Bänder, wichtige Originaldokumente)
- Das Gebäude (z. B. Wände, Fenster) und die Infrastruktur (z. B. Leitungen, Gefahrenmeldeanlagen) werden regelmäßig geprüft und gewartet
- Umzäunung des Betriebsgeländes
- Stabile, einbruchshemmende Fenster und Türen im EG (z. B. nach DIN EN 1627)
- Einsatz von Alarmanlagen zur Einbruchserkennung, insbesondere außerhalb der Arbeitszeit
- Einsatz von Sicherheitspersonal (ggf. extern)
- Einsatz von Videoüberwachungssystemen unter Berücksichtigung datenschutzrechtlicher Anforderungen (Monitoring des Zugangsschutzes)
- Ausreichende Klimatisierung von Serverräumen
- Keine (zu öffnenden) Fenster in Serverräumen
- Einsatz von Anlagen zur Sicherstellung der Stromversorgung von Serversystemen (unterbrechungsfreie Stromversorgung (USV)), insbesondere bei kurzfristigen Stromausfällen oder Schwankungen
- Elementargefahren vorbeugen (insb. Feuer, Rauch, Erschütterungen, chemische Reaktionen, Überschwemmungen, Stromausfälle, Explosionen und Anschläge/Vandalismus)
- Risiken durch Überflutung/Starkregen prüfen, insbesondere bei Serverräumen im Keller oder anderen gefährdeten Bereichen

„Standard"-Maßnahmen zur IT-Sicherheit ist nach Art. 32 DS-GVO für alle verpflichtend.
Einige Maßnahmenempfehlungen sind abrufbar unter
https://www.lda.bayern.de/de/checklisten.html

Heute packen wir aber noch was drauf

yuryimaging@123rf.com

Der wichtigste „Baustein“ dazu:

IT-Administratorin
IT-Administrator

Deep Dive: Höhere Hürden für Angreifer

01 Netzwerksegmentierung umsetzen

- Je größer ein Netzwerk, desto unübersichtlicher wird es
- Es ist häufig nicht erforderlich, dass alle Dienste von jedem Rechner in einem Unternehmensnetz erreichbar sein müssen
- Netzwerksegmentierung schottet interne Netzsegmente (unterschiedlicher Kritikalität/Verwendung) voneinander ab
- Einsatz von Firewalls, Intrusion Detection Systemen und Protokollierung auch innerhalb eines Unternehmensnetzes
- Bei Ransomware: Lateral Movement (Bewegung im Netzwerk) wird massiv erschwert und der Schaden eines Angriffs mitunter deutlich minimiert

Deep Dive: Höhere Hürden für Angreifer

02 Powershell begrenzen

- Windows-Skriptsprachen wir Powershell vereinfachen die Administration teils deutlich
- Diese stehen aber im Zweifel auch Angreifern zur Verfügung, die einen Rechner übernommen haben
- Office-Makros laden gerne über Powershell den richtigen Schadcode nach
- Mit Powershell-Kommandos können ganze Angriffsketten durchgeführt werden – der Virenscanner hat damit meist keine Probleme
- Auch Sicherheitslücken nutzen Powershell-Kommandos gerne direkt aus (z.B. Exchange-Proxyshell zur Fernsteuerung eines Mailservers)
- Deswegen: Powershell auf die Minimalerfordernisse eingrenzen

Deep Dive: Höhere Hürden für Angreifer

03 Programmausführung verhindern

- Ransomware ist auch nur Software –die Softwarekomponenten eines Angriffs werden am besten gar nicht erst ausgeführt
- Sogenanntes „Application Whitelisting“ lässt nur die Ausführung von festgelegten Programmen zu
- Auch sogenanntes „Execution Directory Whitelisting“ verhindert evtl. nicht das Herunterladen eines Schadcodes („Backdoor-Programm“), aber dessen automatische Ausführung
- Damit ist ein Ransomware-Angriff unterbunden und der Virenscanner schlägt vielleicht nach ein paar Tagen dann auch mal an – Glück gehabt.

Deep Dive: Höhere Hürden für Angreifer

04 Fremde Office-Makros unterbinden

- Microsoft Office Software wie Word oder Excel sind komplexe Programm-/Entwicklungsumgebunden, nicht nur schlichte Textverarbeitungsprogramme
- Programmierte Bestandteile (Makros) können im Unternehmensalltag allerlei Aufgaben vereinfachen
- Oder auch Schadcode(„Backdoor-Programme“) automatisch herunterladen und zur Ausführung bringen (mittels Powershell), wenn ein Nutzer nur einmal aus Versehen auf „OK“ klickt
- Jetzt mal Hand aufs Herz: Wer braucht heute noch Office-Makros, die irgendwo aus dem Internet herkommen?
- Deswegen Office-Makros komplett **deaktivieren** oder wenigsten nur die **eigenen** Office-Makros zulassen (sogenannte signierte Makros)

Deep Dive: Höhere Hürden für Angreifer

05 Administrative Passwörter variieren

- Angreifer mit den Benutzerrechten eines „normalen" Mitarbeiters können bei halbwegs ordentlichen Rollen-/Rechtekonzepten nur begrenzten Schaden anrichten
- Deswegen wollen die Angreifer sogenannte privilegierte Rechte erlangen
- Dies sind z.B. lokale Administratorrechte, die auf jedem PC zur Administration vorhanden sind
- Das Problem: Häufig ist das lokale Administratorpassword auf jedem PC das gleiche
- Angreifer freuen sich: Auf einem PC mittels Tools wie Mimikatz ermittelt, steht das gesamte Unternehmensnetz mit Administratorrechten offen
- Die Lösung: Auf jedem PC ein unterschiedliches lokales Administator-Passwort (komfortabel mit Microsofts Tool „Tool „Local Administrator Password Solution")

Deep Dive: Höhere Hürden für Angreifer

06 Internetübergang protokollieren und filtern

- Angreifer kommen meist über das Internet und hinterlassen dabei Spuren
- Häufig werden auch (noch nicht allzulange) bekannte Server von Angreifergruppierungen verwendet
- Dies können Server zum Nachladen von „Backdoor-Programmen“ oder Cloud-Dienste zum Aufschalten auf gekaperte Rechner sein
- Derart bekannte Systeme werden Indictors of Compromise (IOC) genannt, die auch von Sicherheitsprodukten wie Firewalls gepflegt und eingesetzt werden
- Diese verhindern mitunter, das ein Angriff überhaupt erfolgreich sein kann
- Oder zumindest, dass dieser Nachvollzogen werden kann
- Aus Datenschutzsicht interessant: IP-Adressen dürfen nach DS-GVO durchaus für diese Zwecke verarbeitet werden

Deep Dive: Höhere Hürden für Angreifer

07 Air-Gap-Backups einsetzen

- Ransomware-Angreifer wissen, dass es so was wie Backups gibt
- Deswegen wird versucht, ein Backup vor einer Verschlüsselung zu löschen
- Oder die Backups ebenfalls zu verschlüsseln
- Stand der Technik dazu: 3-2-1 Backup-Regel
- Ein Backup sollte dabei nicht mit dem Unternehmensnetz verbunden sein
- Fokus: Backups nicht nur bezüglich einer Ausfallsicherung wie Feuer/Wasser sondern auch mit Blick auf Ransomware-Angreifer denken

Deep Dive: Höhere Hürden für Angreifer

08 Netzwerkkomponenten up-to-date halten

- Cyberangriffe finden nicht nur über Social-Engineering Mails statt
- Manche Gruppierungen verwenden als ersten Angriffsvektor hauptsächlich Sicherheitslücken in Systemen, die über das Internet erreichbar sind
- Beispielsweise Firewalls, VPN-Endpunkte, Fernwartungssysteme, E-Mail und Webserver
- Patch-Management von IT-Systemen ist wichtig. Akribisches Patch-Managment von Netzwerkkomponenten ist aber essentiell
- Auch bedeutsam: Man muss auch wissen, welche Systeme überhaupt vorhanden sind (z.B. hat schon manch eine vergessene ältere Firewall ein Unternehmen innerhalb eines Tages in die Ransomware-Falle tappen lassen)

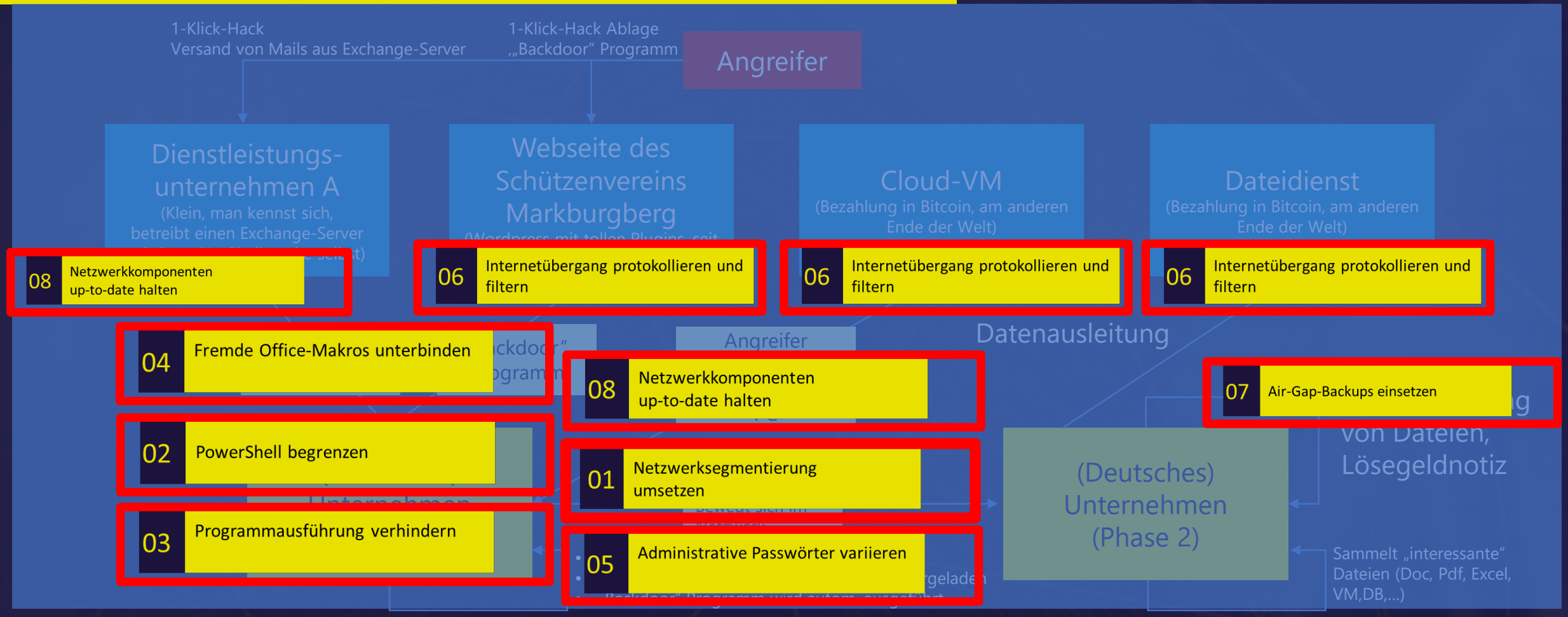
Deep Dive: Höhere Hürden für Angreifer

Acht wirksame Schutzmaßnahmen gegen Ransomware

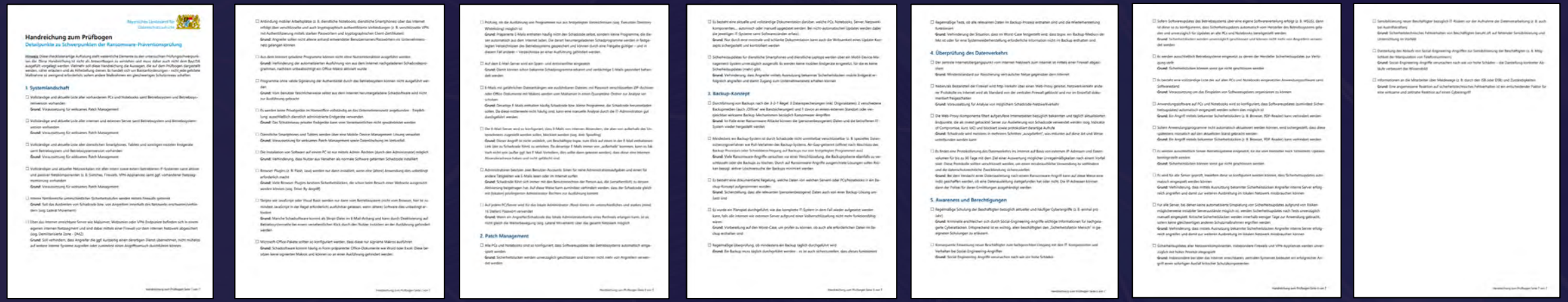
gibt es auch unter https://www.lda.bayern.de/de/cyberpraevention.html

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

Präventionsansatz beim exemplarischen Angriff



Noch mehr Ransomware-Präventionen Maßnahmen?


Handreichung zum Prüfbogen
Detailpunkte zu Schwerpunkten der Ransomware-Präventionsprüfung
1. Systemlandschaft
2. Patch Management
3. Backup-Konzept
4. Überprüfung des Datenverkehrs
5. Awareness und Berechtigungen

https://www.lda.bayern.de/media/pruefungen/Ransomware_Praevention_Handreichung.pdf

Hier nochmals alle momentanen 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

Nun haben wir noch Zeit für Fragen

Vielen Dank für Ihre Aufmerksamkeit.

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