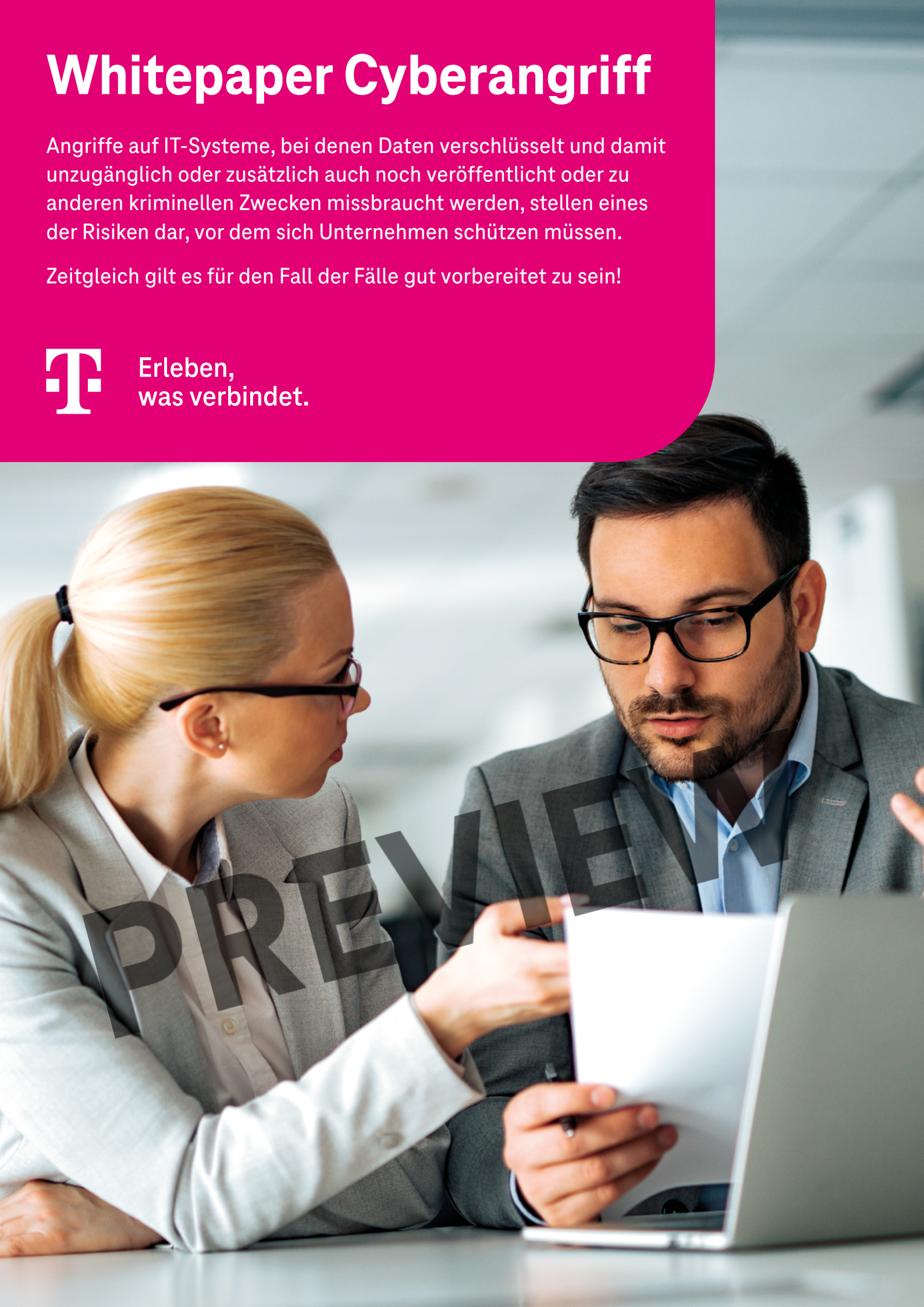
Whitepaper Cyberangriff

Angriffe auf IT-Systeme, bei denen Daten verschlüsselt und damit unzugänglich oder zusätzlich auch noch veröffentlicht oder zu anderen kriminellen Zwecken missbraucht werden, stellen eines der Risiken dar, vor dem sich Unternehmen schützen müssen.

Zeitgleich gilt es für den Fall der Fälle gut vorbereitet zu sein!

Erleben,
was verbindet.



Inhalt

Dieser Leitfaden ist eine Zusammenstellung wichtiger Schritte,

- die als **Sofort-Maßnahmen** empfohlen sind, wenn es zu einem Angriff kommt (s. u. I.),
- die sich als gesetzliche und weitere **Handlungspflichten** an die erste Reaktionsphase anschließen (s.u. II.), und
- die helfen sollen, darüber hinaus entstandene **Schäden zu identifizieren** und zu quantifizieren bzw. ggf. dafür **Regress** zu nehmen (s.u. III.).

Die Liste erhebt nicht den Anspruch auf universelle Anwendbarkeit für alle Unternehmen und alle Branchen oder Situationen und wird auch nicht automatisch aktualisiert. Sie orientiert sich an den Maßstäben und Erfahrungen für Unternehmen in Deutschland.

Die wesentlichen Handlungsempfehlungen sind am Ende dieses Whitepapers als **„Checkliste Cyberangriffe“** zusammengefasst.

I. Sofort-Maßnahmen zur Schadensbegrenzung (Minute 1 – Tag 2)

1. Technische Sofort-Maßnahmen

Sobald sich Unregelmäßigkeiten abzeichnen, die auf einen Cyberangriff deuten, ist schnelle Reaktion gefragt. **Merke: Schnelle und präzise Reaktion statt Panikmodus!**

Wenn möglich: nicht einfach die Systeme panikartig vom Netz nehmen oder Notaus bedienen, sondern **Isolation der befallenen von den noch aktiv erreichbaren Bereichen**. In vielen Fällen löst die Trennung oder der Notaus erst die heimlich eingeschleusten Hintertüren und „Tretminen" der Angreifer aus, wie z. B. die sofortige Komplettverschlüsselung aller Systeme. Die unkontrollierte Netztrennung erschwert zudem ganz erheblich die forensische Aufklärung des Angriffsvektors und der ausgenutzten Lücke im Sicherheitssystem.

Aber: **Verbindungen** zu verbundenen externen Systemen, insbesondere von Kunden, Zulieferern oder Geschäftspartnern sind **so schnell wie möglich zu trennen**, um eine Ausbreitung zu verhindern. Kunden und Partner können sonst nachträglich Schäden wegen Versäumnissen der Schadensminderungspflicht gelten machen. Dabei nur absolute Minimuminformationen nach außen geben: **Keine Kommunikation nach außen ohne Freigabe durch Geschäftsführung, IT Leitung und Datenschutzbeauftragten**. Kommunikation und Transparenz sind wichtig und notwendig, aber auch potentiell gefährlich und schadensträchtig!

Auf keinen Fall: Ungeprüftes Einspielen des Backups der letzten Wochen oder Monate vor dem Erkennen des Cyberangriffs. Im Durchschnitt sind die Angreifer bereits 30 bis 180 Tage heimlich im System gewesen, bevor sie erkannt werden oder sich mit der Verschlüsselung der Daten zu erkennen geben: Genügend Zeit, um alle Backups mit Hintertüren und versteckten Angriffspunkten zu verseuchen. **Backups dürfen nur nach professioneller Prüfung und ggf. Säuberung durch IT-Security Spezialisten eingespielt werden**.

Soweit noch Zugriff auf die IT-Systeme besteht sind folgende Informationen zu beschaffen und **zentral** zu **dokumentieren**:

Logfiles sichern!

a) Schadensursache (Angriffsvektor)

- (Vorsätzliche) Angriffe (Phishing usw.)
- Interne Ursache (Netzwerkfehler, (Schad-)Software, Hardware, usw.)

b) Schadensumfang (Angriffsziele)

- Betroffene Geschäftsbereiche
- Betroffene Systeme
- Betroffene Datenkategorien (Kundendaten, Geschäftsdaten, Betriebsgeheimnisse, Daten von Geschäftspartnern, usw.)
- Art und Weise der Betroffenheit (Verlust von Daten, Preisgabe an Dritte, usw.)

2. Organisatorische Sofort-Maßnahmen

Wer vorgesorgt hat, tut sich auch in der Organisation der Krisenreaktion leichter: Wenn die Standard-Kommunikationskanäle nicht mehr zur Verfügung stehen (E-Mail, Chats, Zugriff auf Telefonnummern, Nutzung von Softphones, digital gespeicherte Notfallpläne etc.), werden alternative Kanäle und Strukturen benötigt. Private Mailboxen und Mobiltelefone sind ein zusätzliches Sicherheitsrisiko, das nur im absoluten Notfall genutzt werden sollte.

Cyberangreifer geben sich oft **kurz vor Wochenende oder Feiertagen** zu erkennen und hoffen auf geringere Aufmerksamkeit und fehlende Verfügbarkeiten der benötigten Ressourcen. Enttäuschen Sie die Angreifer! Legen Sie **analog verfügbare Meldeketten** an, die auch am Wochenende und Feiertag funktionieren, wenn alle digitalen Systeme offline sind. Alle Mitarbeitenden und Partner müssen die eingerichtete Hotline/Meldezentrale kennen, damit potentielle Meldungen schnellstmöglich an die richtige Stelle kommen.

Mindestens ein **vordefinierter Ansprechpartner muss in allen Urlaubs-, Krankheits- und Feiertagszeiten erreichbar sein („First Responder“)**. Ein **Krisenteam** ist schnellstmöglich zu bilden und kommunikativ zu vernetzen. Der First Responder definiert die Rollenverteilung im Krisenteam. Zum Krisenteam gehören mind.: **IT Leitung, Datenschutzbeauftragter, Risikomanager, Unternehmensleitung, Rechtsabteilung, Kommunikationsleitung**.

Das Krisenteam entscheidet über notwendige Erweiterungen durch externe Unterstützung:

- die operative **IT Abteilung**/Leitung hat nicht die Tools, Kenntnisse und Erfahrung zur Verfügung, die professionelle **IT Forensiker und IT-Sicherheitsspezialisten** haben;
- Unternehmenskommunikation ist nicht mit **Krisenkommunikation** zu vergleichen, die viel Erfahrung im kommunikativen Umgang mit Kunden, Medien, Mitarbeitenden, Behörden und Partnern verlangt;
- ein Cyberangriff hat spezifische **rechtliche Handlungspflichten** und Schadensrisiken zur Folge, die nicht unbedingt zum Erfahrungshorizont und Know How Profil der internen Rechtsabteilung gehören.

3. Rechtliche Sofort-Maßnahmen

Das Krisenteam (ggf. mit externer Unterstützung) entscheidet über **sofortige Anzeige- und Meldepflichten** (s.u.) gegenüber Polizei (Cybercrime Einheiten/ZAC), Aufsichtsbehörden (z. B. Datenschutz: innerhalb von 72 Stunden, egal ob Wochenende oder Feiertag, Art. 33 Abs. 1 DSGVO) und internen Aufsichtsgremien. Die rechtzeitige Durchführung wird durch die zuständigen Organe (Datenschutzbeauftragter, Informationssicherheitsbeauftragter etc.) sichergestellt und dokumentiert.

Zentrale Steuerung der Kommunikation ist entscheidend. Keine Kommunikation mit Dritten (z. B. Kunden, Mitarbeitenden, Partnern) oder gar Medien ohne Freigabe des Krisenteams und der Unternehmensleitung.

Das Krisenteam organisiert auch die **sichere Dokumentation und Protokollierung** aller Erkenntnisse und Handlungsschritte sowie den limitierten Zugang dazu. Es besteht eine gesetzliche Pflicht zur Dokumentation nach den Datenschutzgesetzen (Art. 33 Abs. 5 DSGVO) und der Nachweispflicht gegenüber Versicherern. Ohne Dokumentation und Handlungsnachweise drohen erhebliche Schadensrisiken.

Wenn vorhanden ist die **Cyberversicherung oder IT-Haftpflichtversicherung** zu informieren. Bei verspäteter Information droht der Wegfall des Versicherungsschutzes. Die Versicherung kann oft auch erfahrene First Response Teams als externe Unterstützung zur Verfügung stellen.