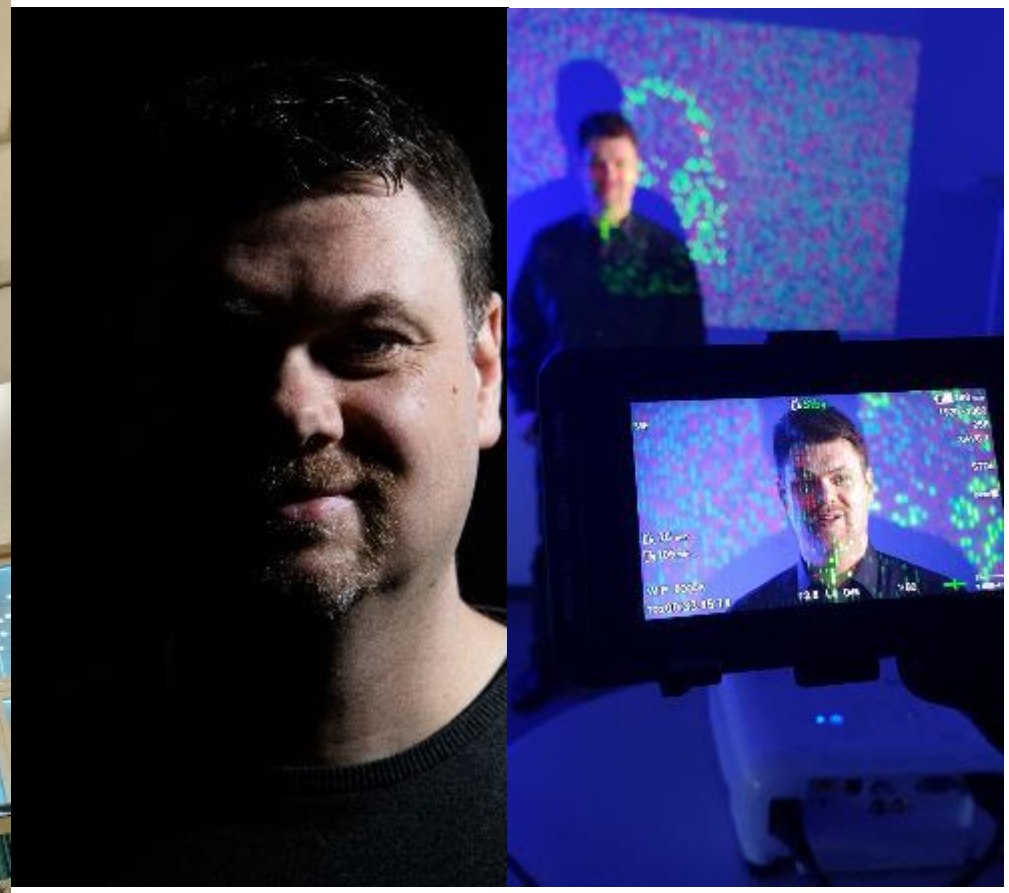
Nikolaus Stapels

Social Engineering

Die Kunst, Menschen digital zu manipulieren



Nikolaus Stapels

- Cyber-Sicherheits-Berater
- VdS-Fachberater für Cyber-Risiken
- Software-Entwicklung
- PenTest
- Incident Response Management

Nikolaus Stapels
Consulting & Training

Linkedin /Xing = Nikolaus Stapels – 04551 – 53 295 79
info@stapels.consulting

Hat Ihnen der Vortrag gefallen?

Dann freue ich mich riesig über eine **Google-Bewertung**! Ihre Meinung hilft anderen – und unterstützt mich dabei, noch mehr Menschen für Cyber-Sicherheit zu begeistern.

https://g.page/r/CWjZ-153t39cEBM/review

Keine Sorge :D

Der Link ist kein Test.

Vielen Dank für Ihre Unterstützung!

Nikolaus Stapels

Interesse geweckt?

Sie möchten wissen, wie wir Unternehmen konkret unterstützen?
Dann werfen Sie einen Blick auf die nächste Folie – dort finden Sie einige unsere **Leistungen** auf einen Blick.

Haben Sie Fragen oder möchten direkt ins Gespräch kommen?

Dann sprechen Sie uns gerne an – **wir freuen uns auf den Austausch!**

Nikolaus Stapels

Cyber Security

360°-Check Ihrer IT-Sicherheit – erkennen Sie Schwachstellen, bevor Angreifer es tun.

Incident Responder

Analyse digitaler Spuren nach einem Vorfall – für rechtssichere Aufklärung und schnelle Reaktion.

PenTest

Unsere Experten prüfen Ihre Systeme gezielt auf Sicherheitslücken – bevor es andere tun.

Cyber-Risk-Score

Ab Oktober 2025 bieten wir eine Lösung, die Ihre IT rund um die Uhr von innen und außen überwacht .

Ransomware-Schutz

Unsere Software erkennt Verschlüsselungsversuche frühzeitig und blockiert sie automatisch.

Darknet Monitoring

Wir überwachen das Darknet auf Hinweise zu Ihrem Unternehmen – diskret und kontinuierlich.

Handout

2026

Einführung

Der Mensch als Zielscheibe

01.

Social Engineering ist der Versuch, Menschen zu täuschen und zu manipulieren, damit sie sensible Informationen wie Passwörter oder vertrauliche Daten preisgeben. Dabei nutzen die Angreifer psychologische Tricks, um das Vertrauen ihrer Opfer zu gewinnen.

02.

Die Angreifer arbeiten oft mit scheinbar harmlosen Anfragen, wie einer dringenden E-Mail oder einem überzeugenden Telefonanruf. Sie spielen dabei mit Emotionen wie Hilfsbereitschaft, Angst oder Vertrauen. Das Ziel ist es, das Opfer dazu zu bringen, ohne nachzudenken sensible Daten preiszugeben

Einführung

Spam und Social Engineering

01. **Spam** bezeichnet **unerwünschte Massen-E-Mails**, die in der Regel Werbung oder betrügerische Angebote enthalten. Sie sind oft generisch und richten sich an eine große Anzahl von Empfängern, **ohne auf eine spezifische Reaktion abzuzielen**. Spam ist meistens leicht erkennbar und relativ harmlos, solange keine Links angeklickt werden.

02. **Social Engineering** hingegen ist **gezielter und viel gefährlicher**. Während Spam darauf setzt, dass jemand zufällig reagiert, ist Social Engineering eine **direkte Manipulation des Opfers**. Die Angreifer täuschen persönliche oder berufliche Beziehungen vor, bauen Vertrauen auf und spielen mit den Emotionen der Zielperson, um gezielt an sensible Informationen zu gelangen.

Vertrauen und Hilfsbereitschaft

Menschen neigen dazu, zu vertrauen und anderen zu helfen, besonders wenn sie denken, dass sie mit einer autorisierten Person sprechen.

Dringlichkeit und Druck

Betrüger erzeugen oft ein Gefühl von Dringlichkeit. Sie sagen zum Beispiel: „Ihr Konto wird gesperrt, wenn Sie nicht sofort reagieren.“

Emotionen und Angst

Angreifer nutzen starke Emotionen wie Angst, um uns dazu zu bringen, Dinge zu tun, die wir normalerweise nicht tun würden.

Einführung

Warum ist Social Engineering so erfolgreich?

Menschliche Faktor

Während technische Schutzmaßnahmen wie Firewalls und Virenscanner immer besser werden, umgehen Social Engineers diese, indem sie direkt den Menschen „hacken“. Eine Sicherheitssoftware kann nicht verhindern, dass jemand freiwillig seine Passwörter herausgibt.

Social Engineering nutzt somit unsere menschlichen Eigenschaften und Schwächen aus – und das macht es so gefährlich. Hier sind die Hauptgründe, warum diese Methode funktioniert:

Einführung

Erfolg von Social Engineering im Detail

1. Vertrauen und Hilfsbereitschaft

Menschen sind von Natur aus sozial und kooperativ. Betrüger wissen das und geben sich oft als vertrauenswürdige Autoritätspersonen aus, wie ein IT-Mitarbeiter oder ein Manager. Durch diese geschickte Tarnung fühlen sich die Opfer verpflichtet, zu helfen – ohne lange nachzufragen. Ein klassisches Beispiel: Jemand ruft an und behauptet, er müsse dringend ein Passwort zurücksetzen, um „Schäden zu vermeiden“. Aus Höflichkeit und dem Wunsch, schnell zu helfen, gibt man ihm die benötigten Daten

2. Dringlichkeit und Druck

Viele Social Engineering-Angriffe erzeugen künstlichen Druck, indem sie eine dringende Situation vortäuschen. Betrüger behaupten oft, dass sofortige Maßnahmen erforderlich sind, etwa durch die Drohung, ein Konto zu sperren oder wichtige Daten zu verlieren, wenn man nicht reagiert. Das Gefühl von Zeitdruck hindert uns daran, ruhig und rational nachzudenken, und wir treffen impulsiv Entscheidungen, die wir unter normalen Umständen vermeiden würden

3. Emotionen und Angst

Emotionen wie Angst und Unsicherheit werden gezielt eingesetzt, um Menschen zu manipulieren. Angreifer nutzen diese Emotionen, indem sie zum Beispiel drohen, dass große Verluste drohen, wenn keine Maßnahmen ergriffen werden. Diese Angst lähmt das rationale Denken und führt dazu, dass Opfer ohne gründliche Überprüfung handeln, um die gefürchteten Folgen zu vermeiden

Einführung

Warum soziale Medien Kriminelle anlocken

Massenhafte Informationen frei verfügbar

Soziale Medien bieten eine riesige Menge an frei zugänglichen Informationen. Laut der ARD-ZDF-Onlinestudie 2023 nutzen **79 % der Deutschen Social Media** regelmäßig. Viele Nutzer geben dort nicht nur private Details wie Geburtstage, Wohnorte und Hobbys preis, sondern teilen auch **berufliche Informationen wie Jobtitel und Projekte**. Diese Informationen sind oft öffentlich zugänglich und ermöglichen es Kriminellen, gezielte Angriffe zu planen

Persönliche Beziehungen ausnutzen

Durch soziale Medien sehen Kriminelle, mit wem das Opfer in Verbindung steht. Dies erleichtert es ihnen, Vertrauen zu schaffen, indem sie vorgeben, ein Kollege oder Geschäftspartner zu sein. Diese Informationen nutzen Angreifer dann für Angriffe wie Spear-Phishing oder Vishing, um sensible Daten zu stehlen.

Täuschung durch Fake-Profile

Ein weiteres Risiko ist die Erstellung gefälschter Profile, die Kriminelle nutzen, um sich als vertrauenswürdige Kontakte auszugeben. Dies geschieht oft auf Plattformen wie z.B. LinkedIn, wo sie sich als Geschäftsleute oder Experten ausgeben und ihre Opfer dazu bringen, sensible Informationen preiszugeben.

Einführung

Verschiedene Arten von Social Engineering

1. Phishing
Kriminelle versenden gefälschte E-Mails, um Benutzer dazu zu bringen, sensible Daten preiszugeben, indem sie auf schädliche Links klicken.

2. Spear-Phishing
Eine gezielte Phishing-Methode, bei der personalisierte E-Mails an eine bestimmte Person oder Organisation geschickt werden, um Vertrauen zu erwecken.

3. Vishing
Kriminelle rufen Opfer an und geben sich als vertrauenswürdige Institution aus, um sensible Informationen wie Passwörter zu erlangen.

4. Smishing
Ähnlich wie Phishing, aber über SMS-Nachrichten, um den Benutzer zu täuschen und vertrauliche Daten zu stehlen.

5. Baiting
Angreifer bieten etwas Verlockendes an (wie kostenlose Downloads), um Opfer dazu zu bringen, Malware herunterzuladen oder persönliche Daten preiszugeben.

6. Pretexting
Der Angreifer erschafft eine falsche Identität oder Geschichte, um das Opfer zu täuschen und an vertrauliche Informationen zu gelangen.

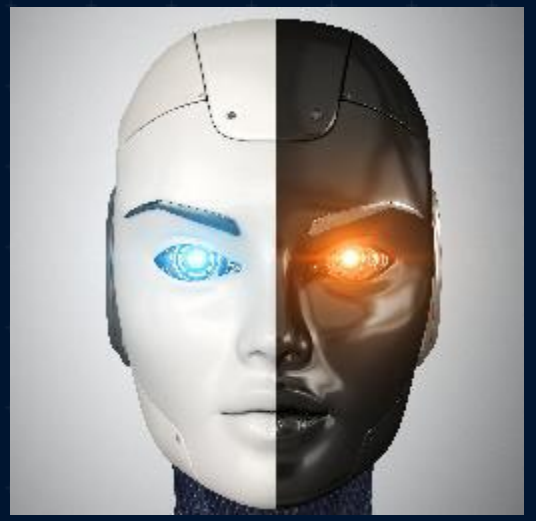
7. Business Email Compromise (BEC)
Kriminelle infiltrieren geschäftliche E-Mail-Kommunikationen oder fälschen diese, um finanzielle Transaktionen zu manipulieren.

Einleitung

Angriffe durch KI

Kriminelle setzen **KI-gestützte Tools** ein, die auf maschinellem Lernen und großen Datenmengen basieren. Das Tool wird gestartet, indem es auf **öffentliche Datenbanken**, **soziale Netzwerke** oder sogar **geleakte Datensätze** zugreift.

Der Angreifer definiert Zielpersonen oder Unternehmen basierend auf bestimmten Kriterien (z. B. Position im Unternehmen, öffentlich zugängliche Informationen). Die KI scannt diese Daten, um mögliche Schwachstellen oder verwundbare Punkte zu identifizieren



Nikolaus Stapels

Social Engineering

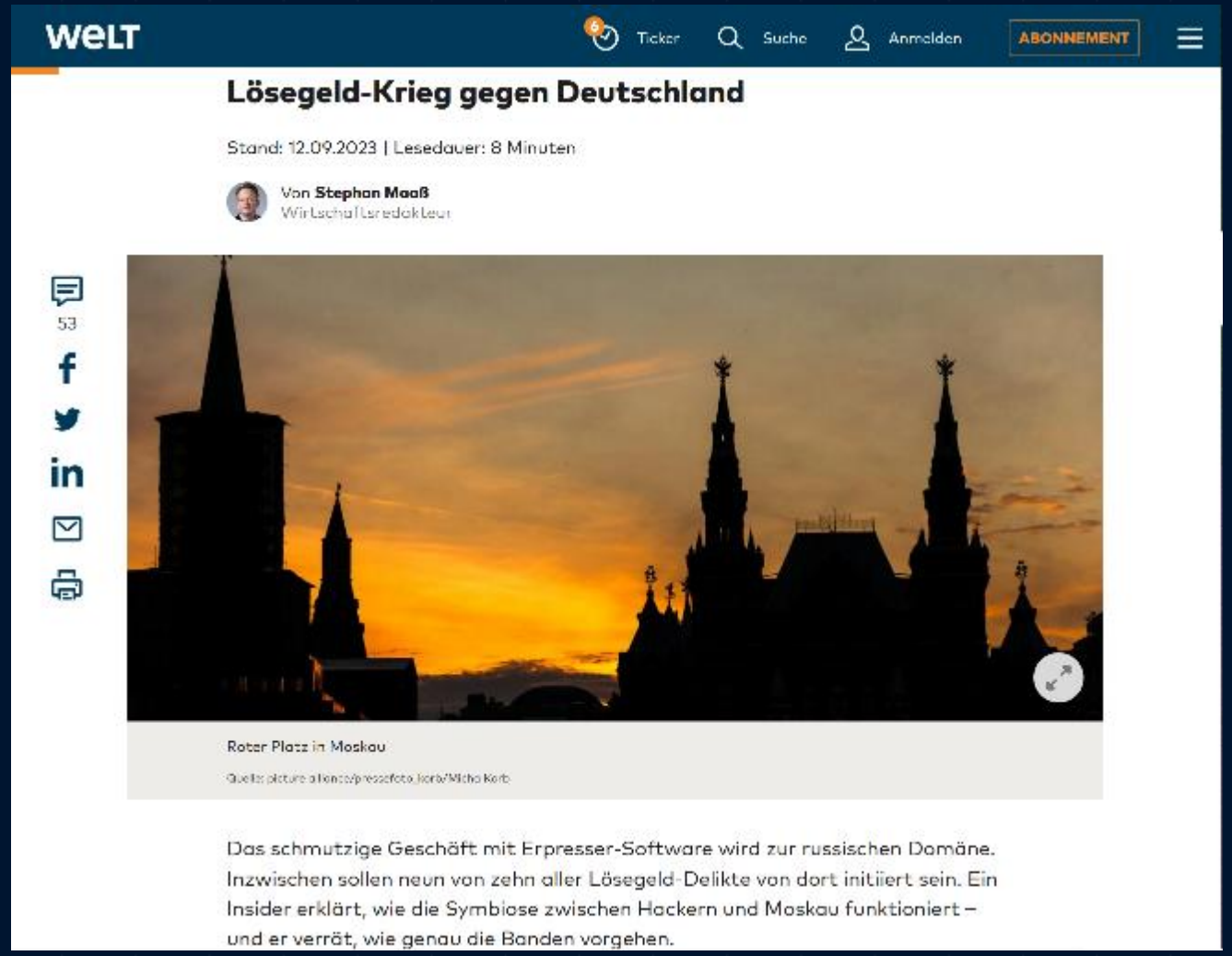
Warum nehmen die Angriffe so zu?

Hintergrund der Angriffe

Cyber Krieg

Die Cybersecurity and Infrastructure Security Agency (CISA) bestätigte, dass russische staatlich geförderte Hacker weiterhin eine bedeutende Bedrohung für kritische Infrastrukturen weltweit darstellen, einschließlich der in Deutschland (CISA).

Diese Angriffe zielen nicht nur auf große Unternehmen, sondern auch auf kleinere und mittelständische Unternehmen, die oft nicht über die notwendigen Ressourcen und das Wissen verfügen, um sich effektiv zu schützen. So soll die wirtschaftliche Entwicklung in Deutschland gestört werden.



WELT Ticker Suche Anmelden ABONNEMENT

Lösegeld-Krieg gegen Deutschland

Stand: 12.09.2023 | Lesedauer: 8 Minuten

Von **Stephan Maaß**
Wirtschaftsredakteur

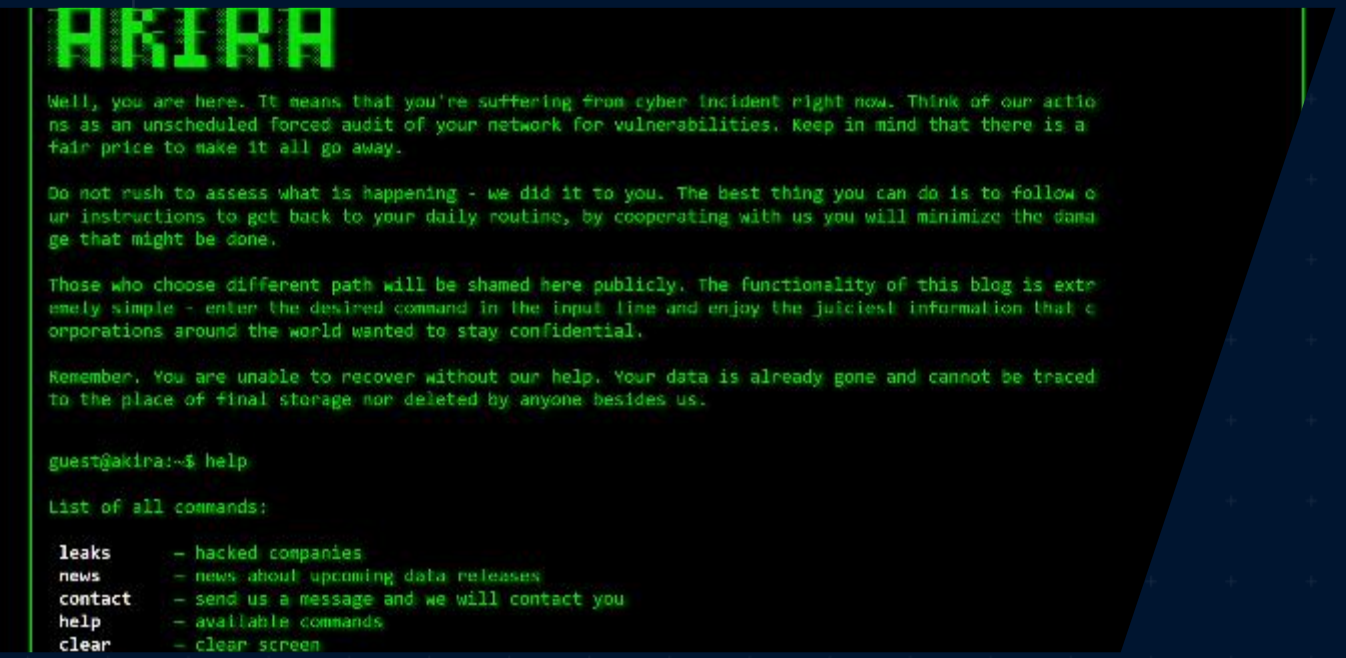
53

Roter Platz in Moskau

Quelle: picture alliance/pressefoto_korb/Micha Korb

Das schmutzige Geschäft mit Erpresser-Software wird zur russischen Domäne. Inzwischen sollen neun von zehn aller Lösegeld-Delikte von dort initiiert sein. Ein Insider erklärt, wie die Symbiose zwischen Hackern und Moskau funktioniert – und er verrät, wie genau die Banden vorgehen.

Akira



NEUES

Diese Gruppe, die sich durch ihre ausgeklügelten Cyberangriffe rasch einen Namen machte und rückte ins Rampenlicht durch den spektakulären Angriff auf die Westfalen IT, bei dem 72 Kommunen betroffen waren.

Ziel von Akira seien immer wieder Server-Systeme, die ohne eine sogenannte Zwei-Faktor-Authentifizierung laufen.

Akira

Wie lautete das Passwort

für die Server der Südwestfalen-IT?

- Admin2354345+#!
- HGtz&%873“§+-=0
- Admin123456
- Admin98765RF$
- 123456

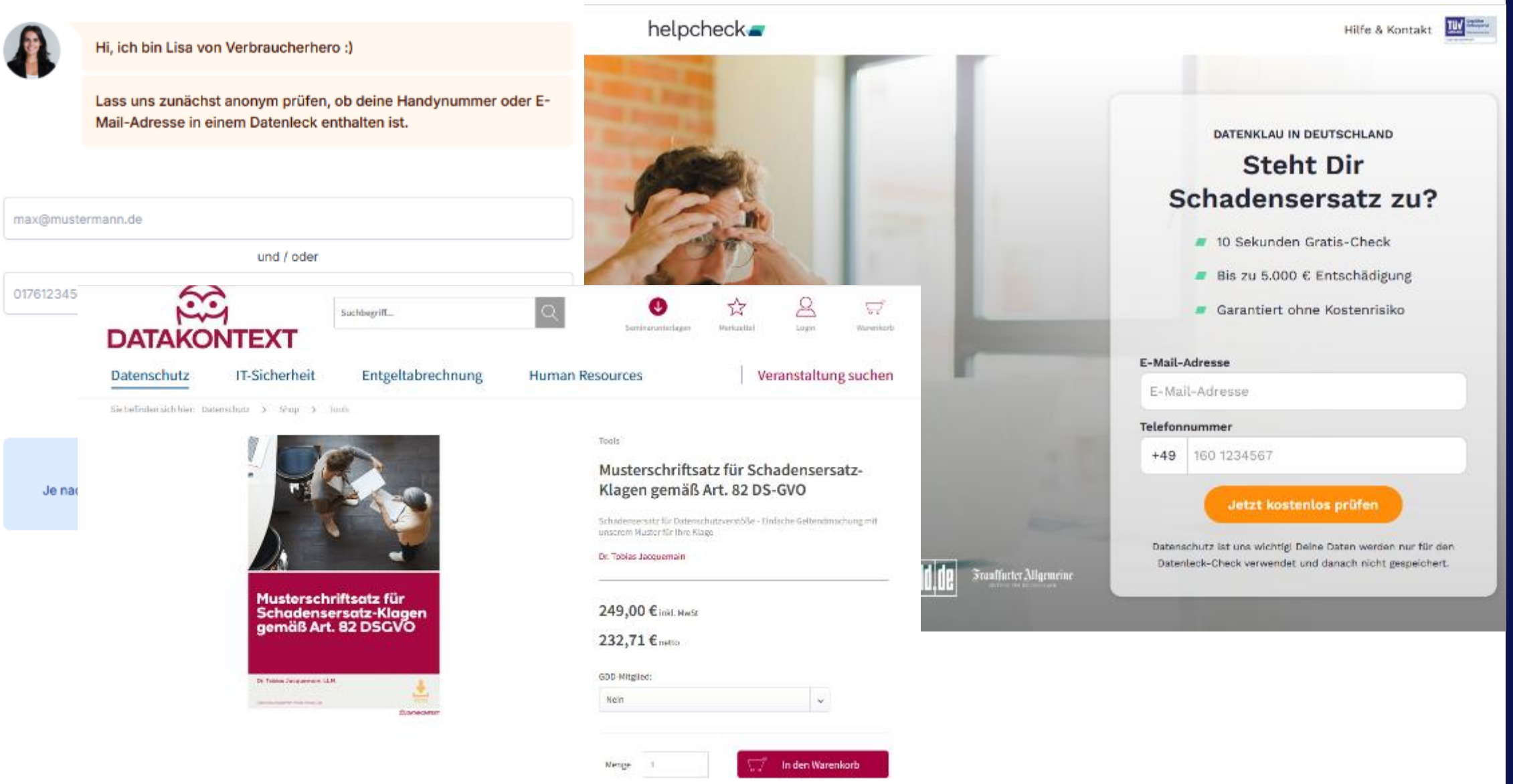
Lockbit

Platz 1

Dank einer einfach zu bedienenden Oberfläche und einer Vielzahl von Funktionen hat LockBit 3.0 den Markt für Ransomware-as-a-Service-Anbieter erobert und war auch in **2025 der führende Anbieter** in diesem Bereich. Dies macht die Bedrohung von Ransomware-Angriffen noch besorgniserregender als zuvor.

Die Prävention ist der beste Schutz gegen Ransomware-Angriffe.

Das Geschäft mit dem Datenleck



Cybercrime Trends 2026

Kriminelle liegen vorne...

Die Innovationskraft der Cyberkriminellen kennt keine Grenzen und ihre Angriffstaktiken sind immer ausgeklügelter. Technische Sicherheitsmaßnahmen reichen oft nicht mehr aus, um diese Trends abzuwehren. Deshalb ist es umso wichtiger, dass die Mitarbeitenden wachsam sind und eine starke Sicherheitskultur etabliert wird.

Cyber-Sicherheits-Team

Die **Erschöpfung** von IT- und Security-Expert:innen stellt für Unternehmen ein wachsendes Problem dar und macht sie anfälliger für Cyberangriffe.

Die **steigende Arbeitsbelastung**, der Mangel an Fachkräften und unzureichende Budgets führen dazu, dass viele Unternehmen unterbesetzte Sicherheitsteams haben, die den Anstieg von Cyberangriffen nicht bewältigen können.

Dies erhöht das Risiko von Fehlern und Schwachstellen in der IT-Sicherheit, die Cyberkriminelle ausnutzen können. Unternehmen sollten die Erschöpfung ihrer Sicherheitsverantwortlichen ernst nehmen und ihnen ausreichende Ressourcen und Unterstützung zur Verfügung stellen, um ihre Motivation und Leistungsfähigkeit zu erhalten.

Ins Unternehmen

Einbruchstore der Cracker

Platz 1
Mails

59%

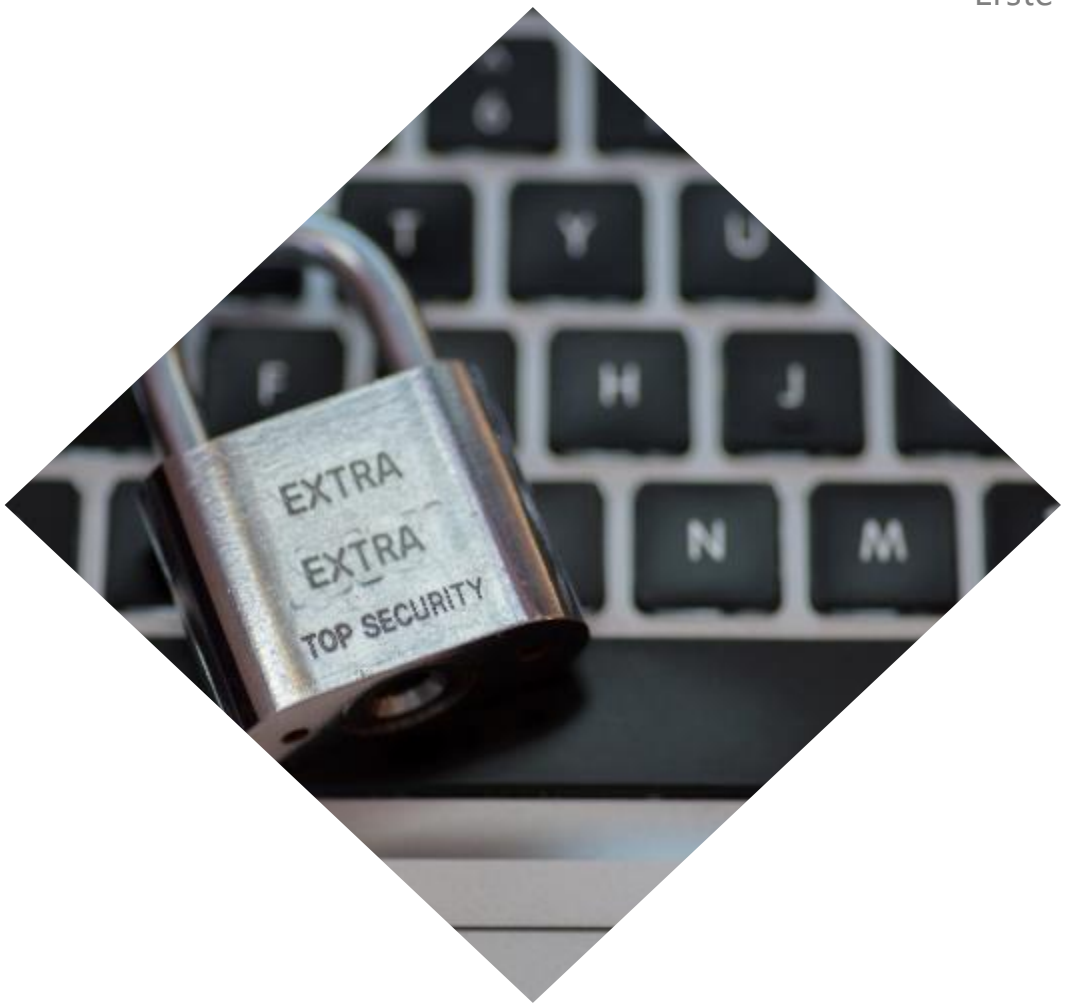
Mitarbeiter, die auf eine infizierte E-Mail klicken oder versehentlich Anmeldeinformationen versenden, sind eine der besten Möglichkeiten für Hacker, Zugang zu Ihrem Netzwerk zu erhalten.

59% der erfolgreichen Angriffe erfolgen über eine Mail.

Die richtige Schulung Ihrer Mitarbeiter kann dagegen helfen, deshalb setzen Versicherer auf Awarenessakademien wie z.B. **den Cyber-Fuchs**.

IT-Sicherheit

Erste Maßnahmen im Unternehmen



- **Festlegung von Sicherheitsrichtlinien**:
  Eine klare und umfassende IT-Sicherheitsrichtlinie ist entscheidend. Sie sollte regelmäßige Passwortänderungen, sichere Passwortgewohnheiten, Verfahren für den Umgang mit sensiblen Informationen und Bestimmungen zum sicheren Umgang mit E-Mails und Internetnutzung beinhalten.

- **Standard-Passwörter ändern**:
  Ändern Sie die Standardpasswörter im Unternehmen, egal ob es bei einem physischen Gerät ist oder einem Online-Dienst. Wichtig ist dies zum Beispiel auch beim WLAN-Router.

- **Verschlüsselung**:
  Die Verwendung von Verschlüsselungstechnologien zum Schutz sensibler Daten, sowohl bei der Übertragung als auch bei der Speicherung, ist von großer Bedeutung.

- **Antivirus- und Antimalware-Software**:
  Alle Systeme sollten mit aktueller Antivirus- und Antimalware-Software ausgestattet sein.

- **Firewalls:**
  Sie dienen dazu, den Zugang zu Netzwerken zu kontrollieren und ungewöhnliche Aktivitäten zu erkennen.

IT-Sicherheit

Erste Maßnahmen im Unternehmen

- **Patch-Management**:
  Sämtliche Software, Betriebssysteme und Anwendungen sollten stets auf dem neuesten Stand sein. Dafür sollte ein effizientes Patch-Management-System implementiert werden.

- **Sicherheitsbewusstseinsbildung und Schulungen**:
  Alle Mitarbeiter sollten über grundlegende IT-Sicherheitspraktiken informiert sein und regelmäßig Schulungen erhalten, um sie auf dem Laufenden zu halten.

- **Backup und Disaster Recovery**:
  Es ist wichtig, regelmäßige Backups aller wichtigen Daten zu erstellen und Pläne für die Wiederherstellung im Falle eines Desasters zu haben. Prüfen Sie auch die Funktionalität Ihrer Datensicherungen.

- **Zugangskontrolle und -verwaltung**: Die Anzahl der Personen mit Zugang zu sensiblen Informationen sollte minimiert werden. Die Nutzung von Zwei-Faktor-Authentifizierung oder Multi-Faktor-Authentifizierung kann dabei helfen.

- **Incident Response Planung**: Ein Plan für den Umgang mit Sicherheitsvorfällen ist unerlässlich, um schnell und effektiv auf mögliche Angriffe reagieren zu können.

Was ist grundsätzlich mitversichert?

Betriebsunterbrechung

Informationskosten

Call-Center

24/7 IT-Forensik

Krisenmanagement

Haftpflicht

PR-Beratung

Kreditkartenüberwachung

Rechtsberatung

„Vertrauensschäden“

Zusammenfassung

Cyber-Absicherungen weiterhin wichtig

Zusammenfassend lässt sich sagen, dass **Cyberkriminelle stetig ihre Fähigkeiten und Taktiken verbessern und anpassen**, um in Kommunen einzudringen und sensible Daten zu entwenden.
Angesichts dieser **wachsenden Bedrohung** ist es für Organisationen unerlässlich, ihre Sicherheitsmaßnahmen kontinuierlich zu überprüfen und zu optimieren. In dieser sich ständig verändernden Bedrohungslandschaft gewinnt eine Cyber-Versicherung zunehmend an Bedeutung, um Unternehmen im Falle eines Cyber-Angriffs finanziell abzusichern und die Folgen solcher Angriffe besser bewältigen zu können.
Kommunen sollten daher nicht nur in ihre technischen Sicherheitslösungen, sondern auch in Cyber-Versicherungen und die Schulung ihrer Mitarbeiter investieren, um ein umfassendes Sicherheitsniveau zu erreichen.