DANIEL ROSSGATTERER · KEYNOTE SPEAKER

DARKNET, HACKER & CO.

Ein Blick hinter die Kulissen von Cyberkriminellen

Wir werden nicht jeden Angriff verhindern.
Aber wir können verhindern, dass aus jedem Angriff eine Krise wird.

Das Wichtigste aus dem Vortrag — zum Mitnehmen und Weitergeben.

DIE LAGE IN ZAHLEN

Was sich gerade verschiebt.

72 Min.

In den schnellsten 25% der Fälle bis zum Datenabfluss.

Im Vorjahr waren es 288 Minuten von der Attacke bis zum Datendiebstahl. Der Domaincontroller fällt nach ø 3,4 Stunden.

---

65 %

Die Identität ist das Einfallstor.

So viele Erstzugriffe laufen über gestohlene Zugangsdaten und übernommene Anmeldesitzungen. Auch MFA ist betroffen.

84,8 %

Angegriffen, bevor ein Patch existiert.

Sie wurden am Tag der Offenlegung (ZeroDay) oder davor angegriffen. Zwei Jahre zuvor waren es 47,9 %.

-23 Std.

Der Angriff beginnt, bevor die Lücke bekannt ist.

So früh wird eine Lücke heute angegriffen. 2025 lag der "Time to Expoint" noch bei 23,2 Tagen - zwischen Lücke und Angriff.

---

26 %

Das Backup ist Teil des Angriffs.

So viele Sicherungen waren vom Angriff selbst betroffen. Nur 41 % konnten daraus wiederherstellen ohne zu zahlen.

10,5 Bio.

US-Dollar Schaden, weltweit, pro Jahr.

Wäre Cyberkriminalität ein Land, hätte sie die drittgrößte Volkswirtschaft der Welt.

---

90 %

Und der wichtigste Wert von allen.

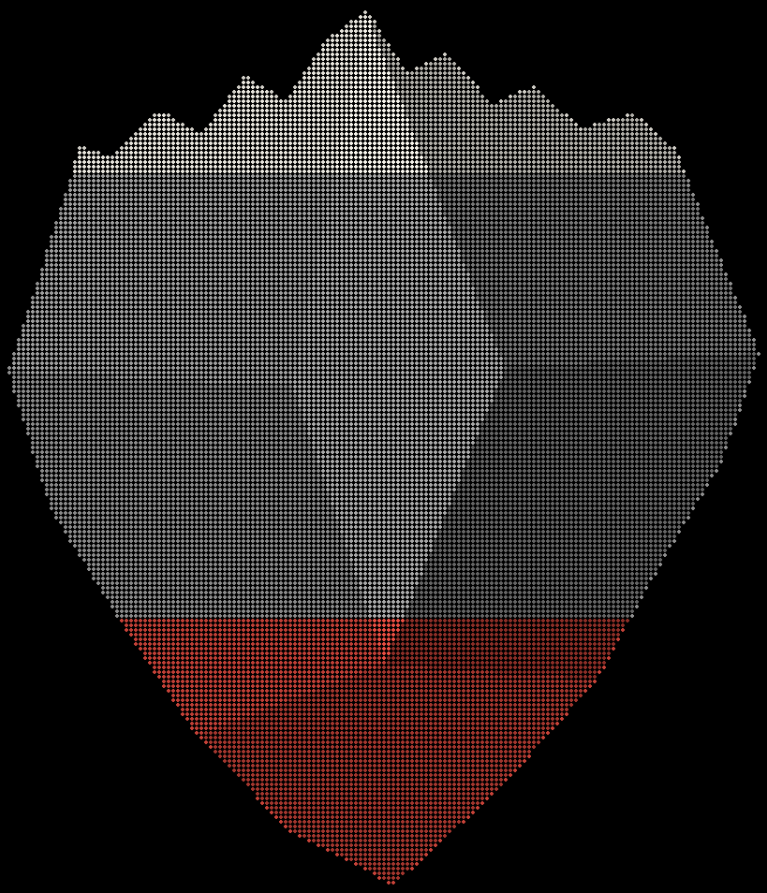
So viele Vorfälle wären vermeidbar gewesen. Durch präventiver Technik und wenigen konsequent umgesetzten Punkten.

EIGENE INCIDENT-RESPONSE-FÄLLE UND BRANCHENAUSWERTUNGEN · STAND 08/2026

Public

DARKNET · EIN BLICK HINTER DIE KULISSEN

Das Internet ist ein Eisberg.



CLEAR WEB ≈ 4–8 %

Das Internet, wie wir es kennen. Sichtbar für alle, erreichbar über Google & Co.

DEEP WEB der große Rest

Alles hinter einer Anmeldung: Onlinebanking, Intranet, Datenbanken, Mail.

DARK WEB die Spitze nach unten

Über das Tor-Netzwerk erreichbar. Anonym, nicht indexiert, keine Suchmaschine.

GOOGLE FINDET NACH GÄNGIGEN SCHÄTZUNGEN 4 BIS 8 PROZENT ALLER INTERNETSEITEN

SPRACHREGIONEN UND DIMENSION

Das Darknet spricht vier Sprachen.

1.000+	2,5 Mio.	täglich
Marktplätze	Nutzer	rund um die Uhr

VIER SPRACHREGIONEN

01 **Russisch**
Die größte Zahl der Ransomware-Gruppen ist russischsprachig. Für uns die wichtigste Region — dort liegen die Informationen, die Unternehmen schützen.

02 **Englisch**
Marktplätze, Foren, Handel mit Daten und Zugängen.

03 **Persisch**
Umgehung von Zensur, politischer Austausch.

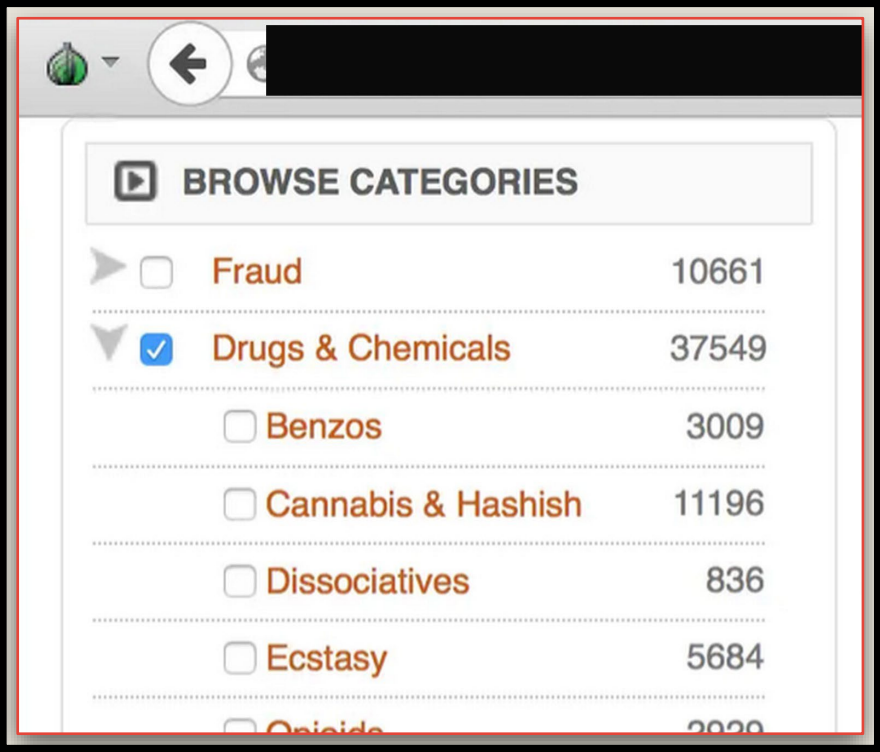
04 **Chinesisch**
Weitgehend abgeschottet, eigene Plattformen.

Das Darknet ist nicht das Problem.

In Ländern mit autoritären Regimen ist es oft der einzige Weg, unzensiert ins Internet zu kommen und sich zu organisieren. Das Problem ist die Anonymität — sie zieht Kriminelle an.

WIE ES DORT AUSSIEHT

Ein Marktplatz wie jeder andere.



37.549 Angebote in einer einzigen Kategorie. 10.661 in einer anderen.

ALPHABAY MARKET · ADRESSE GESCHWÄRZT

Suche, Kategorien, Warenkorb	Bedient wird es wie jeder Onlineshop — keine Spezialkenntnisse nötig.
Händlerbewertungen	Auch hier wird betrogen. Deshalb bewerten Käufer ihre Verkäufer.
Treuhandzahlung	Das Geld wird erst freigegeben, wenn die Ware angekommen ist.

EIGENE RECHERCHE

HACKER · WER DAHINTERSTECKT

Jedes Unternehmen ist angreifbar.

100 %

Diese Frage habe ich einem der besten Penetration Tester gestellt, mit dem wir zusammenarbeiten. Die einzige Frage ist, wie lange es dauert.

Schlecht gesichert: 2 Minuten hinein, 2 Jahre unentdeckt. Sehr gut gesichert: 2 Jahre hinein, 2 Minuten unentdeckt. Dieselben zwei Zahlen, nur vertauscht.

WER ANGREIFT	BEISPIELE	ZIEL
Ransomware-Gruppen	Lockbit, Qilin, Akira. Rund 300 Gruppen, 20 % davon Elite.	Lösegeld
Staatliche Akteure	APT28 „Fancy Bear" — Merkel-Hack. „Sandworm" — Ukraine-Krieg.	Destabilisierung
Politische Gruppen	Anonymous, NoName057. Lose organisiert.	Aufmerksamkeit
Cybercrime privat	Betrug, Erpressung, Social Engineering. Einzeltäter und kleine Banden.	Geld

ANGREIFER SUCHEN KEIN BESTIMMTES ZIEL — SIE SUCHEN AUTOMATISIERT DAS LEICHTESTE

RANSOMWARE ALS GESCHÄFTSMODELL

Drei Rollen. Eine Lieferkette.

JEDER SCHRITT IST EINE DIENSTLEISTUNG

01 **Initial Access Broker — verschafft den Zugang**

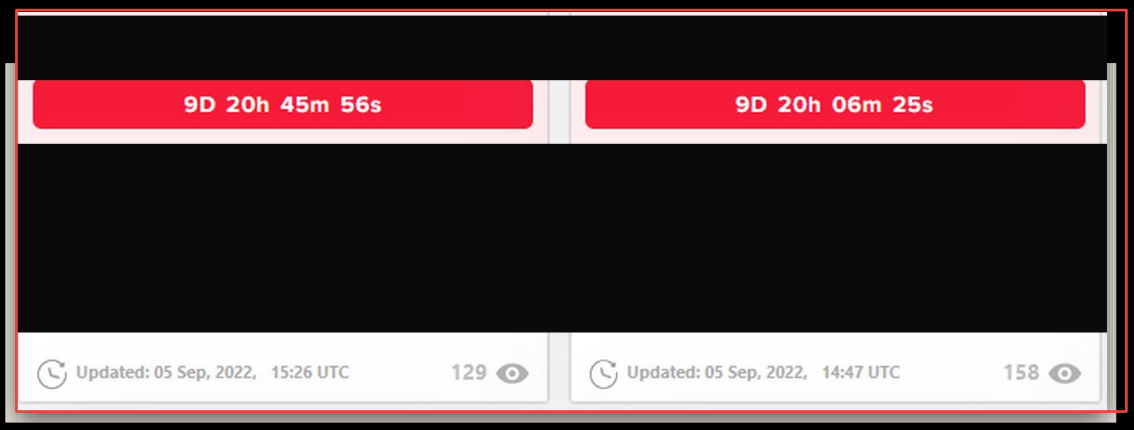
Brute Force, Ausnutzen von Schwachstellen, gezieltes Phishing. Verkauft den fertigen Zugang weiter.

02 **Affiliate — führt den Angriff aus**

Kauft den Zugang, weitet Rechte aus, löscht Backups, zieht Daten ab, verschlüsselt.

03 **RaaS-Betreiber — Plattform und eigene Angriffe**

Baut die Schadsoftware, betreibt die Leak-Seite, legt das Lösegeld fest, greift auch selbst an.



Jedes Opfer bekommt einen Preis und einen Countdown.

LEAK-SEITE EINER RANSOMWARE-GRUPPE · OPFERNAMEN GESCHWÄRZT

Läuft der Timer ab, gehen die gestohlenen Daten online. Genau das macht das Modell so erfolgreich: Die Erpressung funktioniert auch dann, wenn ein Backup existiert.

RANSOMWARE · DER ANGRIFF

Aus 68 Tagen ist ein Arbeitstag geworden.

12–24

Stunden von der Schwachstelle bis zur Verschlüsselung.
2019 waren es 1.637 Stunden, also 68 Tage.
Der Domaincontroller fällt heute nach durchschnittlich 3,4 Stunden.

WAS IM ANGRIFF PASSIERT · DREI HANDGRIFFE

Mehr braucht es nicht.

01 **Backups zerstören**
Es genügt, den Index zu löschen. Die Daten liegen noch da, nur findet sie niemand mehr.

02 **Daten abziehen**
200 GB bis 1 TB verlassen das Haus, bevor irgendetwas verschlüsselt wird.

03 **Daten verschlüsseln**
4 KB pro Datei reichen aus. Deshalb ist der Vorgang in Stunden erledigt.

Erst wird kopiert, dann verschlüsselt. Erpresst wird doppelt.

Deshalb schützt ein funktionierendes Backup zwar vor dem Stillstand, aber nicht vor der Veröffentlichung.

ZAHLEN AUS EIGENEN INCIDENT-RESPONSE-EINSÄTZEN

Public

WIE SIE HEREINKOMMEN

Acht Wege. Aber nur drei Muster.

ÜBER MENSCHEN

Phishing	Frisch registrierte Domains, Anmeldeseiten von Microsoft 365
Abgefangene Anmeldung	Zugangsdaten samt zweitem Faktor
Social Engineering	Gefälschte Stimmen und Videobilder

ÜBER ZUGANGSDATEN

Schadsoftware auf Geräten	Liest Passwörter mit — auf Firmen- wie Privatgeräten
Automatisiertes Durchprobieren	In Wellen nach jedem großen Datenleck

ÜBER TECHNIK UND DRITTE

Schwachstelle ausnutzen	Und eine Hintertür hinterlassen
Über die Lieferkette	Dienstleister und Dienstkonten
Mitlesen der Kommunikation	Mit Schwerpunkt auf Rechnungen

GEGEN DREI MUSTER LÄSST SICH ETWAS TUN — GEGEN ACHT EINZELWEGE NICHT

Public

WENN ES PASSIERT

Die ersten Stunden nach dem Angriff.

SIEBEN SCHRITTE · IN DIESER REIHENFOLGE

01 **Isolieren — aber nicht abschalten**

Vom Netz trennen, nicht herunterfahren. Sonst sind Protokolle, Speicherabbild und Erpresserschreiben weg.

02 **Backups sofort schützen**

Backup-Systeme isolieren, Replikation stoppen, Administratorzugänge absichern.

03 **Krisenorganisation aufsetzen**

Eine Person benennen, die führt. Management, Forensik, Versicherung und Recht über einen sicheren Kanal.

04 **Beweise sichern, Angriff verstehen**

Protokolle, Erpresserschreiben, Warnmeldungen, Speicherabbilder. Umfang, Einstiegsweg und Datenabfluss klären.

05 **Identitäten und Zugänge kontrollieren**

Privilegierte Konten, Sitzungen und Tokens absichern. Fernzugänge prüfen.

06 **Wiederherstellung vorbereiten, nicht blind starten**

Kritische Systeme priorisieren. Erst zurückholen, wenn das System vertrauenswürdig ist.

07 **Parallel mit den Angreifern kommunizieren**

Über einen erfahrenen Verhandler: Zeit gewinnen, den Datenabfluss verifizieren, den Gegner einschätzen.

AUS EIGENEN INCIDENT-RESPONSE-EINSÄTZEN · ZUM AUSDRUCKEN UND AUFHÄNGEN

Public

LÖSEGELD · DIE VERHANDLUNG

Die Summe ist kein Zufall.

48 %

der Unternehmen mit verschlüsselten Daten haben Lösegeld bezahlt.
Gründe: Backup zerstört, kritische Daten, Geschwindigkeit.

5–8 %

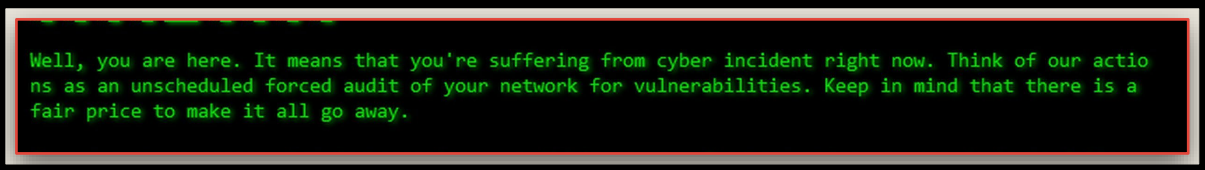
vom Jahresumsatz als Startforderung. Die Forderung deckt sich oft mit den liquiden Mitteln.

WARUM DIE SUMME SO GENAU PASST

01 **Sie kennen Ihre Bilanz**
Jahresabschlüsse sind in vielen Ländern öffentlich.

02 **Sie prüfen Ihre Konten**
Wer mit fehlender Liquidität argumentiert, bekommt seine eigenen Bankauszüge vorgelegt.

03 **Sie fragen nach der Versicherung**
Eine aktive Cyberversicherung wird im Erpresserschreiben ausdrücklich abgefragt.



So empfängt die Leak-Seite das Opfer.

AKIRA · LEAK-SEITE IM TOR-NETZWERK

SECUTEC VERHANDLUNGEN · SOPHOS STATE OF RANSOMWARE 2026 · UNIT 42 GLOBAL IR REPORT 2026

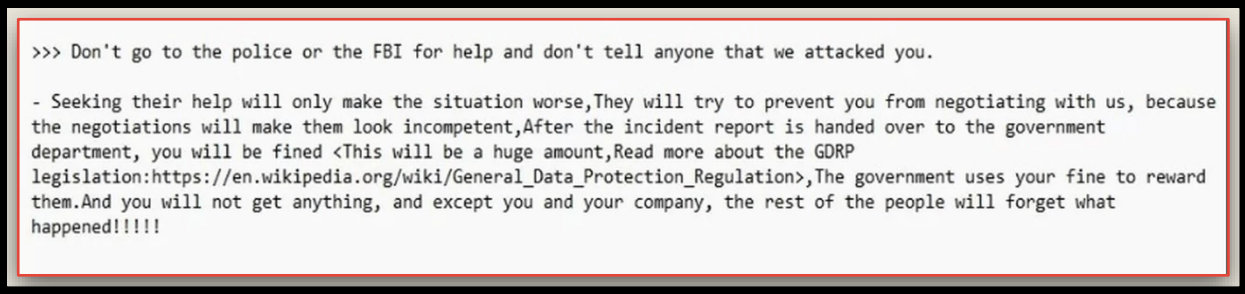
DAS ERPRESSERSCHREIBEN

„Hi friends."

> „Lassen Sie uns die Tränen und den Groll erst einmal für uns behalten und versuchen, einen konstruktiven Dialog aufzubauen."

> „Wir sind nicht daran interessiert, Sie finanziell zu ruinieren."

> „Wenn Sie eine aktive Cyber-Versicherung haben, lassen Sie es uns wissen, und wir werden Ihnen zeigen, wie Sie diese richtig nutzen können."



>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.

- Seeking their help will only make the situation worse,They will try to prevent you from negotiating with us, because the negotiations will make them look incompetent,After the incident report is handed over to the government department, you will be fined <This will be a huge amount,Read more about the GDRP legislation:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>,The government uses your fine to reward them.And you will not get anything, and except you and your company, the rest of the people will forget what happened!!!!!

ORIGINAL · ERPRESSERSCHREIBEN · „GEHEN SIE NICHT ZUR POLIZEI"

Das ist der einzige Rat, den Sie auf keinen Fall befolgen sollten.

Begründet wird er damit, dass Behörden die Verhandlung stören und ein Bußgeld drohe. Tatsächlich gilt die Meldefrist von 72 Stunden nach der Datenschutz-Grundverordnung — und die Behörden sind Teil der Lösung, nicht des Problems.

VORBEREITUNG SCHLÄGT VERHANDLUNG

Klären Sie das, bevor es passiert.

SECHS FRAGEN · HEUTE BEANTWORTEN, NICHT IM ERNSTFALL

01 **Wer entscheidet über eine Zahlung?**
Namentlich, mit Vertretung.

02 **Deckt die Versicherung das ab?**
Und ab wann muss sie informiert werden?

03 **Wer verhandelt?**
Ein eingespielter Verhandler, kein eigener Mitarbeiter.

04 **Wie kommunizieren wir?**
Ein zweiter Kanal, unabhängig vom eigenen Netz.

05 **Welche Daten schmerzen?**
Wer das vorher weiß, verhandelt besser.

06 **Wie schnell sind wir wieder zurück?**
Diese Zahl ist Ihre Verhandlungsposition.

Wer diese sechs Fragen vorher beantwortet hat, verhandelt aus einer Position.

WAS ZU TUN IST · TEIL 1 VON 2

Früh verhindern. Schnell erkennen. Schaden begrenzen.

FÜR DAS UNTERNEHMEN · FÜNF PRIORITÄTEN

Technikunabhängig. In dieser Reihenfolge.

01 **Sehen, was Angreifer sehen**

Angriffsfläche, Darknet und geleakte Zugangsdaten beobachten. Gefährliche Domains und Verbindungen früh blockieren.

02 **Identitäten härten**

Starke Mehrfaktor-Anmeldung oder Passkeys, Phishing-Erkennung. Erweiterte Rechte nur, wenn sie gebraucht werden.

03 **Lücken schließen**

Kritische Schwachstellen schnell beheben, Sichtbarkeit nach außen reduzieren. Zugänge von Cloud, Lieferanten und Dienstleistern kontrollieren.

04 **Erkennen und stoppen**

Auffälliges Verhalten zentral überwachen, Anomalien erkennen. Systeme schnell isolieren, Netze segmentieren.

05 **Widerstandsfähig bleiben**

Sicherungen getrennt und unlöschbar aufbewahren. Wiederherstellung, Krisenplan und Handlungsanweisungen regelmäßig testen.

AUS VORFÄLLEN, IN DENEN VERMEIDBARE LÜCKEN DEN ANGRIFF ERST MÖGLICH GEMACHT HABEN

Public

WAS ZU TUN IST · TEIL 2 VON 2

Im Zweifel: Stoppen. Prüfen. Melden.

FÜR MITARBEITENDE · FÜNF GEWOHNHEITEN

Gilt für jede Rolle, nicht nur für die IT.

01	**Anmeldungen**	Passwortmanager nutzen, nicht im Browser speichern. (NordPass, Keeper, 1Password)
02	**Anfragen**	Dringlichkeit ist ein Warnsignal. Bei ungewöhnlichen Anweisungen nachfragen.
03	**Daten und KI**	Nur freigegebene Programme und KI-Dienste. Vertrauliches bleibt intern.
04	**Geräte**	Privates und Berufliches trennen. Bildschirm sperren, nichts unbekanntes installieren.
05	**Melden**	Verdächtiges sofort melden - auch nach einem Fehlklick.

IM PRIVATEN BEREICH · FÜNF DINGE

Gute Gewohnheiten schlagen komplizierte Technik.

01	**Konten**	Passwortmanager nutzen, nicht im Browser speichern. Mehrfaktor (MFA) aktivieren.
02	**Geräte**	Updates automatisch installieren — auch Router und Smart Home.
03	**Sicherung**	Wichtige Daten getrennt sichern und die Wiederherstellung testen.
04	**Betrug**	Zeitdruck ist ein Warnsignal. Auch Kinder und Großeltern darauf ansprechen.
05	**Geld und Daten**	Bankgeschäfte nur über offizielle Apps. Kartendaten sparsam speichern.

Public

VERNETZEN WIR UNS

Danke.

Ich untersuche Cyberangriffe, verhandle mit Erpressern und erzähle auf der Bühne, was dabei wirklich passiert. Wenn Sie Fragen zum Vortrag haben oder über einen Auftritt sprechen wollen, melden Sie sich gern.

LINKEDIN
Daniel Rossgatterer

SPEAKER-SEITE
danielrossgatterer.com

Dieses Handout darf frei weitergegeben werden.