WENN ALLES STILLSTEHT

Reagieren statt resignieren

CAIRO

1. Der Albtraum beginnt

> *„Wir haben ein Problem – die Produktion steht still.“*
>
> *Donnerstag, 05.56 Uhr. Ein mittelständischer Produktionsbetrieb*

- Kein Zugriff auf das SAP-System
- Kein Etikettendruck
- Maschinensteuerung funktioniert nicht

Diagnose: Da stimmt was nicht 😩

CAIRO

Die IT wird verständigt

Die interne IT oder der IT-Dienstleister wird über den Ausfall informiert.

Um 6 Uhr morgens manchmal nicht ganz so einfach 😉

- Erste Analyse: Ist es ein lokales Problem oder systemweit?
- Überprüfung: Netzwerkanbindung, Serververfügbarkeit, Zugriffsrechte

Noch wissen wir nicht, was los ist.

Auffälligkeiten erkannt Dateien mit .akira-Endungen

Eine akira_readme.txt liegt auf dem Desktop.

CAIRO

Hallo Freunde,

Egal, wer Sie sind und welche Position Sie innehaben – **wenn Sie das hier lesen, bedeutet das, dass die interne Infrastruktur Ihres Unternehmens vollständig oder teilweise tot ist. Alle Ihre Backups – virtuelle, physische – alles, was wir erreichen konnten – wurden vollständig entfernt.** Zudem haben wir **eine große Menge Ihrer Unternehmensdaten vor der Verschlüsselung kopiert.**

Nun, lassen wir fürs Erste alle Tränen und den Groll beiseite und versuchen wir, **einen konstruktiven Dialog aufzubauen.** Uns ist vollkommen bewusst, welchen Schaden wir durch die Sperrung Ihrer internen Systeme verursacht haben. Im Moment sollten Sie Folgendes wissen:

1. Wenn Sie mit uns kooperieren, **sparen Sie VIEL Geld,** denn **wir sind nicht daran interessiert, Sie finanziell zu ruinieren.**
Wir werden Ihre **Finanz-, Bank- und Einkommensunterlagen, Ihre Ersparnisse, Investitionen usw.** genau analysieren und Ihnen **eine angemessene Forderung** unterbreiten.
Wenn Sie über eine **Cyberversicherung** verfügen, teilen Sie uns das mit – **wir zeigen Ihnen, wie Sie diese korrekt nutzen.**
Wenn Sie die Verhandlungen in die Länge ziehen, wird das zum Scheitern des Deals führen.

2. Wenn Sie mit uns kooperieren, **sparen Sie ZEIT, GELD und AUFWAND** und sind **innerhalb von ca. 24 Stunden wieder einsatzfähig.**
Unser Entschlüsselungsprogramm funktioniert bei allen Dateien oder Systemen einwandfrei – Sie können es testen, indem Sie einen **Test-Decryption-Service** gleich zu Beginn der Kommunikation anfordern.
Wenn Sie versuchen, Ihre Systeme eigenständig wiederherzustellen, bedenken Sie bitte:
Sie können dauerhaft den Zugriff auf einige Dateien verlieren oder diese beschädigen – in diesem Fall **können wir nicht helfen.**

3. Der **Sicherheitsbericht** oder **exklusive Insiderinformationen**, die Sie **nach einer Einigung** erhalten, **sind äußerst wertvoll,**
da **kein vollständiges Audit Ihrer Systeme** zeigen wird, **auf welchem Weg wir in Ihr Netzwerk gelangt sind.**
Wir zeigen Ihnen die Schwachstellen, die wir ausgenutzt haben, um Zugang zu erhalten, Sicherungslösungen zu identifizieren und Ihre Daten hochzuladen.

Oha – Der Hacker wird zum IT-Sicherheitsberater 🤩

4. Was Ihre Daten betrifft:
Wenn wir uns nicht einigen, werden wir **persönliche Informationen / Geschäftsgeheimnisse / Datenbanken / Quellcode verkaufen** –
im Grunde alles, was auf dem Darknet von Wert ist – und zwar an **mehrere Bedrohungsakteure gleichzeitig.**
Dann wird **alles auf unserem Blog veröffentlicht** – **https://akira[.]onion**

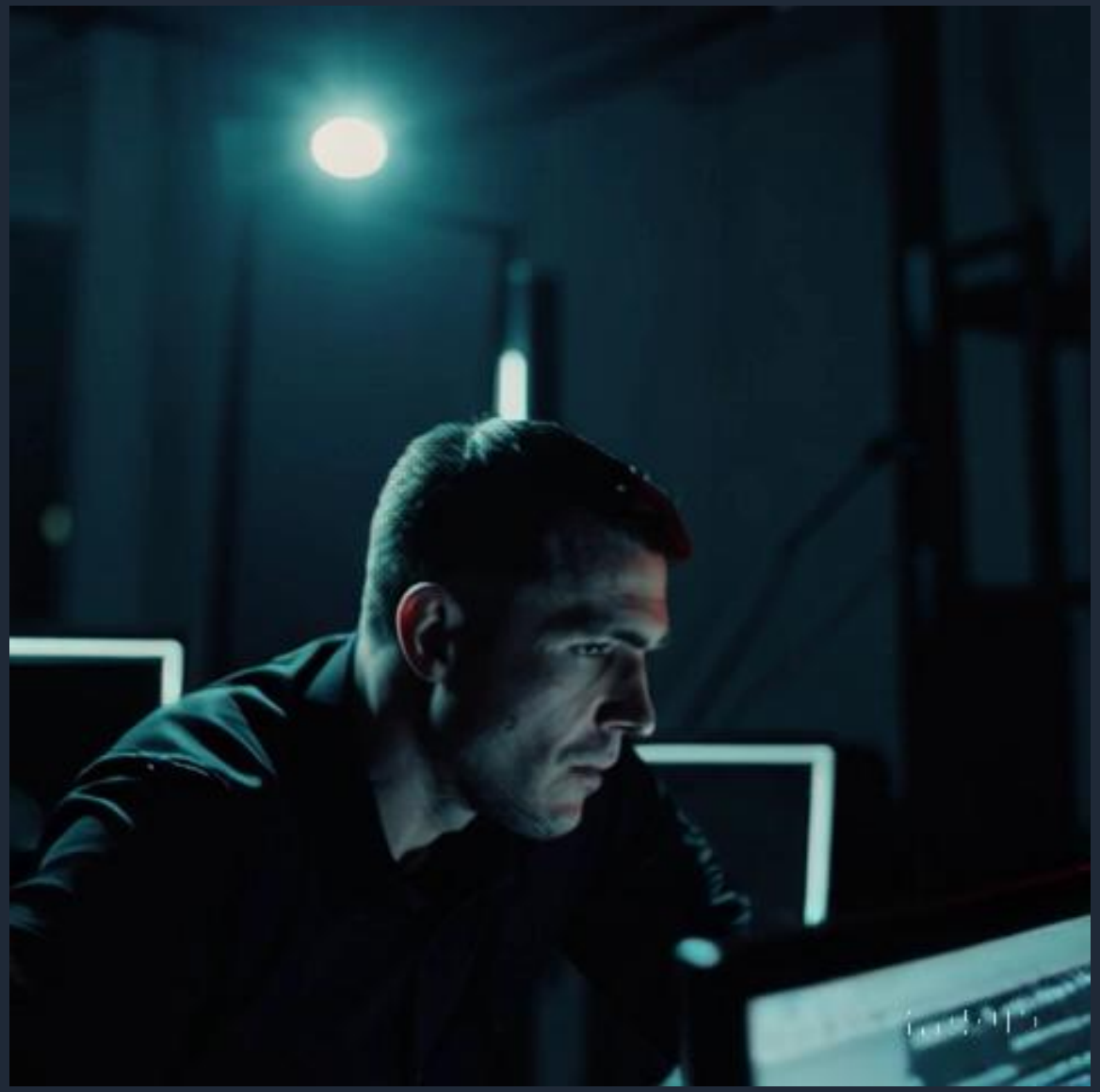
5. **Wir sind äußerst verhandlungsbereit** und werden **ganz sicher eine Lösung finden, die für beide Seiten akzeptabel ist.**

War ein Scherz – sie sind nicht nett!

Spätestens jetzt ist klar

Houston – we have problem!

Zeit den Notfallplan zu aktivieren!



CAIRO

Phase 1: Sofortmaßnahmen

Überlegt Handeln und cool bleiben

1. **ISOLIEREN**
   ALLE Systeme vom Netzwerk trennen.

2. **AKTIVIEREN**
   Internes Notfallteam einberufen.

3. **SPERREN**
   Remote-Zugänge (VPN, RDP) blockieren.

4. **DOKUMENTIEREN**
   Jede Entscheidung, jede Maßnahme protokollieren.

CAIRO

Die entscheidende Frage

Hast du eine Cyberversicherung?

VS

Ohne Versicherung

Auf sich allein gestellt
Operativer & finanzieller Kampf
Hohes Existenzrisiko

Mit Versicherung

Professionelle Hilfe auf Abruf
Strukturierter Krisenstab
Gesteuerte Reaktion

CAIRO

Weg ohne Versicherung: Der Kampf an allen Fronten

Operativ und finanziell komplett auf sich alleine gestellt.

- ❌ Panische Suche nach teuren Experten
- ❌ Interne Überlastung des Teams
- ❌ Volles Kostenrisiko für das Unternehmen
- ❌ Riskante, ungeschützte Verhandlungen

Resultat: Eine potenzielle Existenzbedrohung

CAIRO

Weg mit Versicherung: Der Krisenstab steht bereit

Du bist nicht allein. Die Versicherung agiert als Dein Generalunternehmer in der Krise.

- ✅ Incident Response Management
- ✅ Forensik-Spezialisten
- ✅ Ransomware-Verhandlungsführer
- ✅ Riskante, ungeschützte Verhandlungen
- ✅ Juristen & PR Berater
- ✅ Kostenübernahme (gemäß Police)

CAIRO

Wichtig: Die Versicherung gibt nicht nur – sie fordert auch!

Der häufigste Fehler: Eigenmächtiges Handeln

Wer selbstständig Systeme wiederherstellt, mit Erpressern verhandelt oder Forensiker beauftragt, riskiert seinen Versicherungsschutz

Phase 3: Forensik & Beweissicherung

Den digitalen Tatort sichern

- **Eintrittstor finden**
  Wie kamen die Angreifer ins Netzwerk?
- **Bewegungen nachvollziehen**
  Welche Systeme sind betroffen?
- **Datenfluss analysieren**
  Welche Daten wurden gestohlen?
- **Eintrittszeitpunkt feststellen**
  Wann kam der Angreifer zum ersten Mal ins Netzwerk?

Grundsatz: Nichts verändern bevor die Spurensicherung abgeschlossen ist!

Wichtige Info: Alle Systeme sind bis zur Freigabe durch die Forensik gesperrt!

CAIRO

Phase 4: Prüfung des Backups

Die Millionen-Euro-Frage: Sind unsere Rettungsbote seetüchtig?

- **Identifikation**
  Gibt es Backups, die von der Infizierung nicht betroffen sind?
- **Verifizierung**
  Sind die Backups wirklich sauber?
- **Geduld**
  Voreilige Rücksicherung führt ggf. zu Neuinfektion!

Ein kompromittiertes Backup ist kein Rettungsanker, sondern eine Zeitbombe

CAIRO

Phase 5: Kommunikationsstrategie

Kontrolliere lieber Du die Erzählungen, bevor sie dich kontrollieren

INTERN

- Sachlich, ehrlich, transparent
- Klare Anweisungen geben
- Panik vermeiden

EXTERN

- Proaktiv, kontrolliert, abgestimmt
- Vertrauen bei Kunden & Partnern erhalten
- Meldepflichten (DSGVO, BSI) erfüllen

CAIRO

Phase 6: Wiederherstellung & Härtung

Chance nach der Krise: Sicherer Neuaufbau statt einfacher Wiederherstellung

1. **NEUAUFBAU**
   Systeme aus garantiert sauberen Quellen neu installieren
2. **HÄRTUNG**
   Identifizierte Schwachstellen systematisch schließen (MFA, Ports, etc.)
3. **LEASONS LEARNED**
   Organisatorische und technische Lehren ziehen.

Nicht einfach den alten Status wiederherstellen

CAIRO

Die wichtigste Lektion

Ein Angriff ist kein Zufall.

Vorbereitung ist der beste Schutz.

> *„Kein Unternehmen ist ‚zu klein' oder ‚zu uninteressant'."*

*Ein strukturierter und geübter Notfallplan ist der Unterschied zwischen einem Betriebsausfall **von Stunden** und einem **von Wochen oder Monaten**.*

CAIRO

Fazit: Resilienz beginnt vor dem Angriff

Nicht die Bedrohung entscheidet über den Ausgang, sondern die Reaktion darauf.

Unsere Empfehlung – werdet jetzt aktiv:

- ✅ **Etabliert einen getesteten Notfallplan (kontaktiert uns gerne hierzu)**
- ✅ **Schult das Schlüsselpersonal regelmäßig (auch hierbei können wir helfen)**
- ✅ **Schließt eine passende Cyberversicherung ab (am Besten bei Sven Linke 🧭)**
- ✅ **Arbeitet mit erfahrenen Incident Response Partner zusammen (CAIRO 😎)**

CAIRO

Fragen & Antworten

Vielen Dank für Eure Aufmerksamkeit!

CAIRO

secure • digital • IT-infrastructures

Marcus Düsi
CEO
marcus.duesi@cairo.ag
+49 621 8675142

CAIRO AG
Hermsheimer Str. 3
68163 Mannheim

www.cairo.ag
linkedin.com/in/duesi

CAIRO