



Securing
Your Digital
World

infoGuard
SWISS CYBER SECURITY

Cyber-Notfall live: Strategien, Entscheidungen, Konsequenzen

Interaktive Cyberkrisensimulation – InfoGuard AG



Agenda

- Begrüßung und Einführung
- Hintergrund & Kontext
- Live-Cyberangriff – Simulation
- Szenarien & Entscheidungsfindung
- Auswertung & Learnings
- Abschluss & Fragenrunde

Cyberkriminalität – Ein Big-Business

IT **INSIDE IT**

INSERIEREN JOBPORTAL EVENTS REPORTS ▾

TECHNOLOGIE PARTNER

DEEPImpact

GOLD SPONSOREN



AUSZEICHNUNGEN





Ransomware-Lösegeld knackt erstmals die Milliarden-Marke

Von [Philipp Anz](#), 8. Februar 2024 um 11:25

SECURITY CYBERANGRIFF RANSOMWARE STUDIE CHAINALYSIS



Cybercrime To Cost The World \$10.5 Trillion Annually By 2025

June 16, 2022

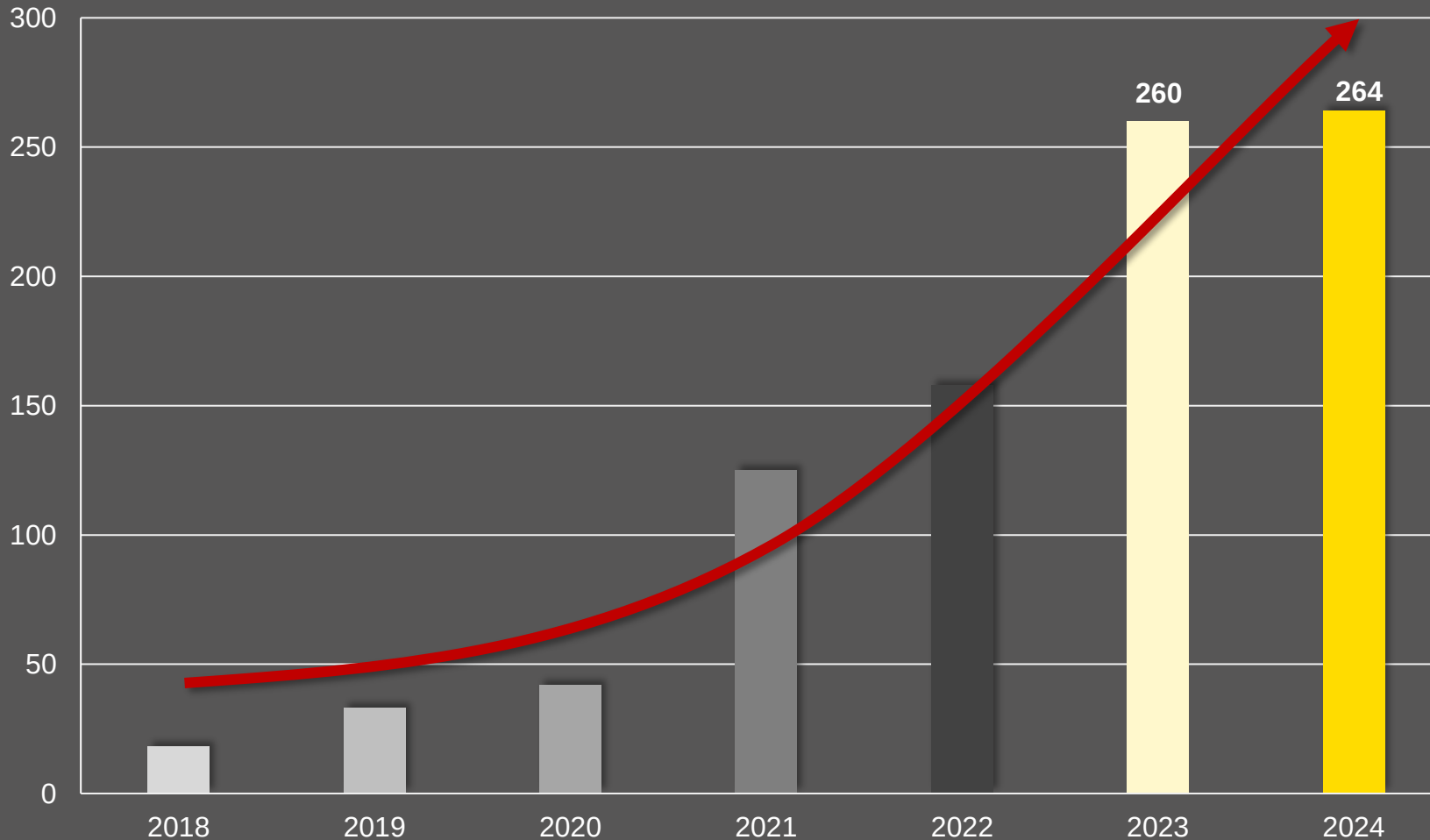
In this article you will learn about how much cyber crime can cost a company. Cybercrime is predicted to inflict \$6 trillion USD in damages globally in 2021, and will reach \$10.5 trillion USD annually by 2025, an

≡ **CNN World** Africa Americas Asia Australia China Europe India Middle East

Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'

InfoGuard Computer Security Incident Response Team

CSIRT Vorfälle 2018-2024



**Hohe Fallzahlen ermöglichen
tagesaktuelle Informationen
über die Bedrohungslage.**

Geschäftsmodell Cyber Crime



REMOTE ACCESS
BROKER



INITIAL ACCESS
BROKER



RANSOMWARE
AFFILIATES



RANSOMWARE
OPERATORS /
DEVELOPERS



Mask	Country	State / City	Details	Info	Vendor	Blacklist	Price	Action
195.141.**** ISP: Sunrise Communications AG		Zurich Zurich	OS: Win2008/7 Proc: Intel Core i7 7840K RAM: 6 GB 16.71 / 73.13 Mbit/s	Admin: No Paypal: No NAT: No	de####ok [platinum]		\$ 6.00	
178.192.**** ISP: Swisscom (Schweiz) AG - Bluewin		Lucerne Emmenbruecke	OS: Windows Proc: - RAM: - GB - / - Mbit/s	Admin: - Paypal: - NAT: -	RDP [platinum]		\$ 10.00	
188.61.**** ISP: Swisscom (Schweiz) AG - Bluewin		Zurich Zurich	OS: Windows Proc: - RAM: - GB - / - Mbit/s	Admin: - Paypal: - NAT: -	RDP [platinum]		\$ 10.00	
83.79.**** ISP: Swisscom (Schweiz) AG - Bluewin		Ticino Locarno	OS: Windows Proc: - RAM: - GB - / - Mbit/s	Admin: - Paypal: - NAT: -	RDP [platinum]		\$ 10.00	
81.6.**** ISP: green.ch AG		Lucerne Eich	OS: Win2008/7 Proc: Intel/Amd RAM: 2 GB 1 / 1 Mbit/s	Admin: No Paypal: Yes NAT: Yes	JS####ow [platinum]		\$ 6.00	
20.199.**** ISP: Microsoft Corporation		Zurich Zurich	OS: Windows Proc: - RAM: - GB - / - Mbit/s	Admin: - Paypal: - NAT: -	RDP [platinum]		\$ 10.00	
46.140.**** ISP: UPC Schweiz GmbH		Geneva Carouge	OS: Windows Proc: - RAM: - GB - / - Mbit/s	Admin: - Paypal: - NAT: -	RDP [platinum]		\$ 10.00	
109.164.**** ISP: Swisscom (Schweiz) AG - Cybernet		Solothurn Deitingen	OS: Win2008/7 Proc: - RAM: - GB - / - Mbit/s	Admin: No Paypal: - NAT: -	am####mg [platinum]		\$ 6.00	

Simulierter Cyberangriff – Überblick

- Diese Übung dauert etwa **45 Minuten**.
- Wir gehen ein **simuliertes Angriffsszenario** durch. Eine Person bringt unerwartete Ereignisse („Injects“) in den Ablauf ein.
- Bei jedem Ereignis müssen die Teilnehmer **Fragen beantworten**. Die Rollen wechseln im Verlauf der Übung.
- Die **Antworten werden anonym erfasst** und auf dem Bildschirm visualisiert.
- Handeln Sie so, wie Sie es in einem echten Sicherheitsvorfall tun würden.
- Das InfoGuard **Expertenteam gibt Ihnen Feedback** basierend auf den Ereignissen und Entscheidungen.

Entscheidungsfindung im Krisenfall

- Wer übernimmt die **Verantwortung für die Reaktion** auf den Vorfall?
- **Wer ist** in den einzelnen Phasen **entscheidungsberechtigt**?
- Wie organisieren Sie die **Koordination zwischen den externen Stakeholdern**?
- Wie koordinieren Sie die **Zusammenarbeit der internen Stakeholder**?
- Wie behalten Sie die **Kontrolle über den Informationsfluss** zwischen den Beteiligten und Dritten?
- Müssen verschiedene **rechtliche Vorgaben** eingehalten werden?
- Gibt es unterschiedliche **Prioritäten für die Reaktion**?

Hintergrundinfos zur fiktiven Firma SecureBank AG

Unternehmensprofil:

- Internationale Bank mit Hauptsitz in Frankfurt
- Geschäftsaktivitäten in 8 Ländern (Europa & Asien)
- Über 6.000 Server, darunter Windows und Linux
- Virtualisierte Infrastruktur und Cloud-Dienste
- ca. 20.000 Mitarbeiter, überwiegend mit Windows-PCs ausgestattet
- Nutzung von Active Directory



INJECT 1

2. Mai

17:09



Inject 1 – Erste Systemanomalien

Meldung

Mehrere Mitarbeiter berichten über stark verlangsamte Systeme und kurzfristige Ausfälle kritischer Anwendungen.

Rolle

Helpdesk-Manager

Frage

Melden Sie den Vorfall sofort an das zentrale Sicherheitsteam?

- A. Ja
- B. Nein
- C. Nur zur Information



INJECT 2

8. Mai

09:09



Inject 2 – Externe Warnung

Meldung

Eine staatliche Behörde weist auf ungewöhnlichen Datenverkehr zwischen einer bekannten Hacker-IP und Ihren öffentlichen IP-Adressen hin.

Rolle

CISO

Frage

Wer sollte in diesem Moment die Reaktion leiten?

- A. Netzwerkteam
- B. SOC
- C. Krisenstab



INJECT 3

8. Mai

16:34



Inject 3 – EDR-Alarm

Meldung

Ihr EDR meldet eine „high severity“-Warnung: Ein neuer Exploit, der Microsoft Office angreift, wurde entdeckt.

Rolle

SOC-Manager

Frage

Wie priorisieren Sie diesen Vorfall?

- A. Kritisch
- B. Mittel
- C. Niedrig
- D. Abwarten, da es nur ein Einzelfall zu sein scheint



INJECT 4

9. Mai

14:19



Inject 4 – Infizierte Endgeräte

Meldung

Die Analyse zeigt, dass mehrere Endgeräte mit einer fortgeschrittenen Remote-Access-Malware kompromittiert sind.

Rolle

CIRT

Frage

Welche Sofortmaßnahmen leiten Sie ein?

- A. Isolation der betroffenen Systeme
- B. Neuformatierung der Systeme
- C. Weitere Untersuchung



INJECT 5

9. Mai

16:28



Inject 5 – Kompromittierte Administratorzugänge

Meldung

Ungewöhnliche Aktivitäten im Administratorbereich und Hinweise auf kompromittierte VPN-Zugänge sorgen für Alarm.

Rolle

CIO

Frage

Leiten Sie zu diesem Zeitpunkt die Prozesse für einen schwerwiegenden Sicherheitsvorfall ein?

- A. Ja
- B. Nein



INJECT 6

12. Mai

13:56



Inject 6 – Erweiterte Systeminfektion

Meldung

Weitere 23 Systeme senden Daten an einen bekannten Command-and-Control-Server, darunter ein Domain Controller, und zwei VPN-Konten wurden infiltriert.

Rolle

CIRT

Frage

Wer sollte in Ihrem Unternehmen die Reaktion leiten?

- A. SOC/CIRT
- B. Unternehmensführung
- C. Rechtsberater
- D. Krisenstab bzw. Business-Continuity-Team



INJECT 7

12. Mai

20:19



Inject 7 – Ungewöhnliche Logins

Meldung

Logdateien des Primary Domain Controllers zeigen, dass sich außerhalb der Geschäftszeiten jemand mit den Anmeldedaten des kompromittierten Administratorkontos eingeloggt hat.

Rolle

Rechtsabteilung

Frage

Sind Sie verpflichtet, diesen Vorfall zu melden?

- A. Ja, und ich kann die entsprechenden Verpflichtungen benennen
- B. Nein, zum jetzigen Zeitpunkt nicht
- C. Die Angaben reichen nicht aus, um eine Entscheidung zu treffen
- D. Ich müsste zunächst die betroffenen Daten analysieren



INJECT 8

15. Mai

19:02



Inject 8 – Angriff über vertrauenswürdigen Serviceprovider

Meldung

Die Analyse des betroffenen Administratorkontos zeigt, dass ein schädliches Word-Dokument – über einen vertrauenswürdigen Serviceprovider – eingeschleust wurde.

Rolle

Vendor Manager

Frage

Wie gehen Sie mit dem Serviceprovider um?

- A. Den Anbieter benachrichtigen und um weitere Informationen bitten
- B. Mit dem zuständigen Kollegen sprechen
- C. Domain/IP-Adresse des Serviceproviders blockieren
- D. Erst abwarten und nichts unternehmen



INJECT 9

15. Mai

10:13



Inject 9 – Ransomware Clap entdeckt

Meldung

Im Intranet wurde ein legitimes Dokument gefunden, das modifiziert wurde und nun die Ransomware Clap enthält, die komplette Systeme löschen kann.

Rolle

CIRT

Frage

Welche Maßnahmen leiten Sie ein?

- A. Die Datei löschen
- B. Alle zugehörigen Domains/IP-Adressen blockieren
- C. Das betroffene System zeitweise vom Netzwerk trennen
- D. Zunächst weiter untersuchen, bevor Maßnahmen ergriffen werden



INJECT 10

17. Mai

07:42



Inject 10 – Kommunikationskrise und Notfallreaktion

Meldung

Angesichts der Verbreitung der Ransomware Clop planen Sie die nächsten Schritte im akuten Krisenfall.

Rolle

Alle involvierten Teams

Frage

Wie gut ist Ihr Unternehmen auf derartige Maßnahmen vorbereitet?

- A. Wir haben einen Notfallplan und Checklisten, die wir sofort nutzen können
- B. Wir würden das schon irgendwie hinkriegen
- C. Es gibt teilweise definierte Prozesse, aber nicht für alle Maßnahmen
- D. Wir wären völlig unvorbereitet

Was genau ist passiert?

Zusammenfassung des Vorfalls – Was genau ist passiert?

- Ein technisch versierter Angreifer hat sich Zugang zum internen Netzwerk verschafft.
- Dazu hat er zunächst einen Serviceprovider infiltriert, von dem die Firma Managed Services bezieht, und diesen als Ausgangspunkt für einen Spear-Phishing-Angriff auf das Unternehmen missbraucht.
- Das Opfer des Spear-Phishing-Angriffs war ein Domain-Administrator, der ein schädliches Word-Dokument geöffnet hat.
- Dieses Dokument enthielt ein Makro, das Malware in den Arbeitsspeicher geladen und das System infiziert hat.
- Da die Malware nie auf einer Festplatte gespeichert wurde, konnte die Antiviren-Software sie nicht finden.
- Sobald der Angreifer sich Zugang verschafft hatte, begann er, die interne Infrastruktur auszuspähen.
- Dabei wurden auch Daten (z. B. Anmeldedaten für Active Directory) gestohlen und ein Backdoor eingerichtet
- Außerdem schleuste der Angreifer die Ransomware Clop in die Umgebung ein, um sie dort für die spätere Nutzung zu verbreiten.

Worüber sie nachdenken sollten

- Wer übernimmt die Verantwortung für die Reaktion auf einen Vorfall?
- Wer ist in den einzelnen Phasen entscheidungsberechtigt?
- Wie organisieren Sie die Koordination zwischen den externen Stakeholdern?
- Wie koordinieren Sie die Zusammenarbeit der internen Stakeholder?
- Wie behalten Sie die Kontrolle darüber, welche Informationen die verschiedenen beteiligten Gruppen untereinander austauschen und an Dritte weitergeben?
- Müssen Sie verschiedene rechtliche Verpflichtungen und Vorgaben erfüllen?
- Gibt es unterschiedliche Prioritäten für die Reaktion?

Drei zentrale Learnings:

1. Klare Eskalations- und Kommunikationswege: Wer ist wann und wie informiert?
2. Schnelle, koordinierte Reaktion: Die Wichtigkeit eines effektiven Notfallmanagements.
3. Kontinuierliche Verbesserung: Regelmäßige Überprüfung und Anpassung der Sicherheitsstrategien basierend auf den Simulationsergebnissen.

7-Punkte-Plan für den Notfall

1. Richten Sie einen Krisenstab ein.
2. Planen Sie regelmässige Sitzungen.
3. Kommunizieren Sie regelmässig.
4. Denken Sie an Meldepflichten.
5. Holen Sie sich frühzeitig externe Unterstützung
6. Stellen Sie Ihre Handlungsfähigkeit wieder her.
7. Vergessen Sie die Nachbearbeitung nicht.



Whitepaper-Download



Professionelle Unterstützung bei einem Sicherheitsvorfall



Angriff

Übernahme / Coaching
Krisenstab

Forensische
Untersuchung

Eindämmung der
Situation

Behörden

Verhandlung mit
Erpressern

Rechtliche
Unterstützung

Krisen-
kommunikation

Unterstützung
bei Bezahlung

Learnings &
Verbesserung



Schutz vor einem Geschäftsausfall

Gesicherter Wiederanlauf / Aufbau





Securing
Your Digital
World

infoGuard
SWISS CYBER SECURITY

Cyber Security ist unsere Leidenschaft

Securing Your Digital World – 360° Cyber Security

InfoGuard
SWISS CYBER SECURITY



2001

Erfahrung und
Expertise seit
über 24 Jahren

100 Mio.

CHF Umsatz

100%

eigenständig

350+

Sicherheitsexperten

17 Lernende

6

Standorte in Baar,
Bern, Frankfurt,
München, Düsseldorf
und Wien

24/7

Echtzeitüberwachung
und Notfallintervention

SOC in CH & DE

24/7 Security Operations Center in der
Schweiz und Deutschland

**CSIRT
Computer Security
Incident Response Team**

BSI-qualifizierter APT-Response-Dienstleister
und FIRST-Mitglied

**ISO 27001
ISO 14001
ISAE 3000 Typ 2**

InfoGuard – 360° Cyber Security

InfoGuard
SWISS CYBER SECURITY





InfoGuard CYBER DEFENCE CENTER



2xSOC

24/7 Security
Operations Center
in der Schweiz
und Deutschland

90+

Experten im
SOC & CSIRT

400+

CDC- & CSIRT-
Kunden

13+

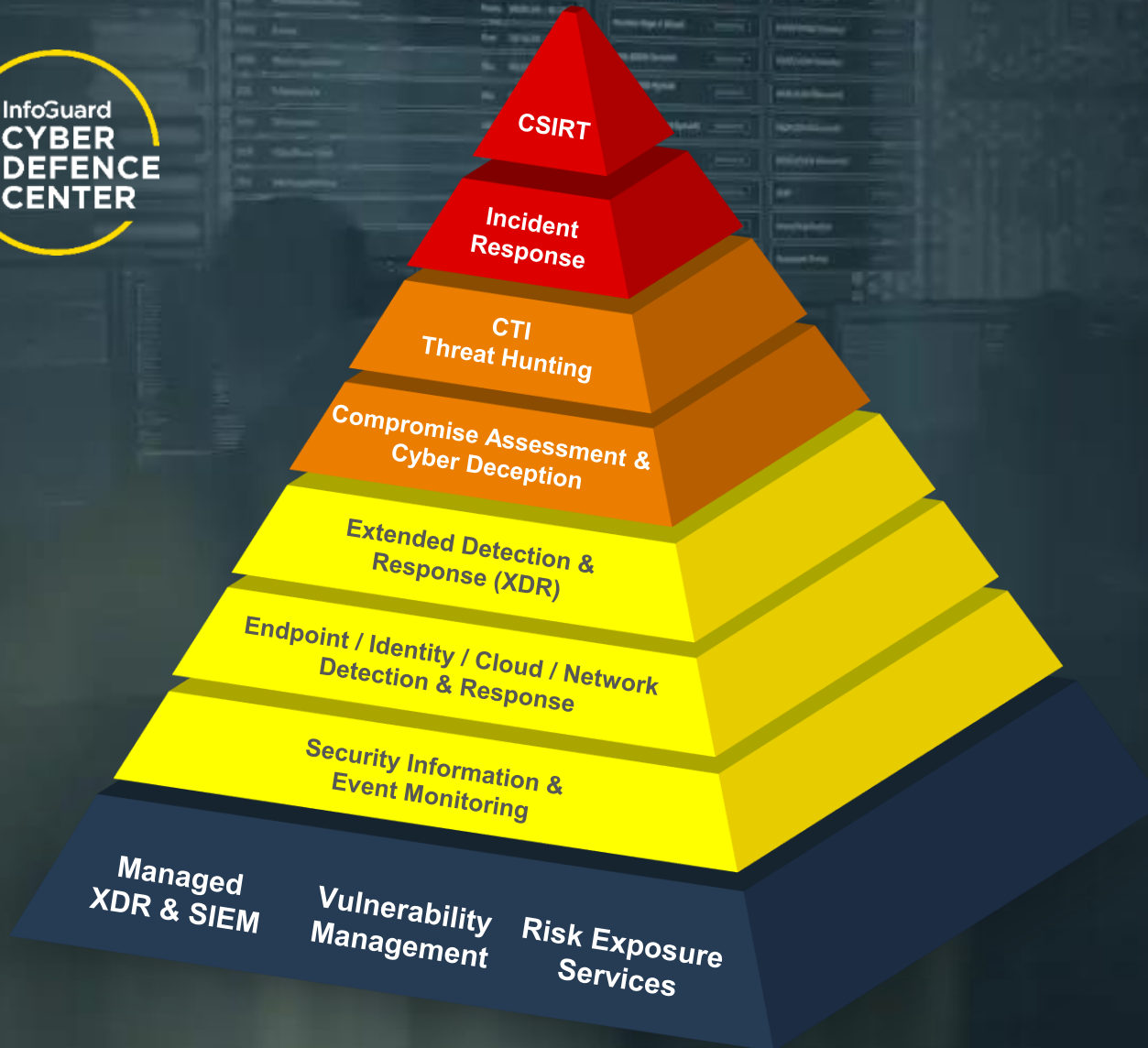
Jahre Erfahrung &
SOC-Kompetenz

ISO 27001
ISO 14001
ISAE 3000 Typ2

CSIRT
Computer Security
Incident Response Team

BSI-qualifizierter APT-Response-
Dienstleister und FIRST-Mitglied

24/7 Cyber Defence & Incident Response Services – Umfassender Schutz vor Cyberangriffen



CSIRT

INCIDENT RESPONSE & RECOVERY

- Incident Response / CSIRT
- Forensics
- Crisis & Incident Response Readiness

MDR

HUNTING & INTELLIGENCE

- Cyber Threat Intelligence (CTI)
- Threat Hunting
- Compromise Assessment
- Cyber Deception

MANAGED DETECTION & RESPONSE

- Extended Detection & Response (XDR)
- Endpoint & Identity Detection & Response (EDR & IDR)
- Cloud & Network Detection & Response (CDR & NDR)
- Security Information & Event Monitoring (SIEM)

MSS

SECURITY OPERATIONS

- Managed XDR & SIEM
- Vulnerability Management
- Digital Risk Exposure Services

InfoGuard CSIRT – Rund um die Uhr für Sie da



24/7 Hotline

 **+41 41 749 19 99**

 **+49 896 142 9677**

 **+43 1 442 0177**

E-Mail

 **investigations@infoguard.ch**

 **investigations@infoguard.de**

 **investigations@infoguard.at**

InfoGuard
SWISS CYBER SECURITY

InfoGuard – Ganz in Ihrer Nähe

InfoGuard
SWISS CYBER SECURITY



Baar (Hauptsitz)

InfoGuard AG
Lindenstrasse 10
6340 Baar / Schweiz

Tel: +41 41 749 19 00
www.infoguard.ch

Bern

InfoGuard AG
Stauffacherstrasse 141
3014 Bern / Schweiz

Tel: +41 31 556 19 00
www.infoguard.ch



Frankfurt

Com-Sys GmbH
Frankfurter Straße 233
63263 Neu-Isenburg / Deutschland

Tel: +49 6102 7840 0
www.com-sys.de

München

InfoGuard Deutschland GmbH
Landsberger Straße 302
80687 München / Deutschland

Tel: +49 896 142 9660
www.infoguard.de

Düsseldorf

Com-Sys GmbH
Am Gierath 20A
40885 Ratingen / Deutschland

Tel: +49 2102 5789 800
www.com-sys.de

Wien

InfoGuard GmbH
Graben 19
1010 Wien / Österreich

Tel: +43 1 442 0170
www.infoguard.at

Securing Your Digital World – Today and Beyond

InfoGuard GmbH

Graben 19

1010 Wien / Österreich

T +43 1 442 0170

info@infoguard.at

www.infoguard.at

Andreas.Senn@infoguard.at