Agentur Cyberschutz

Agentur Cyberschutz

GESAMTKONZEPTE GEGEN CYBERCRIME

ganzheitliche, umfassende IT- und Cybersicherheit

für alle Branchen und Unternehmensgrößen

Oliver HIETZ

Keynote-Speaker - Kriminal-Analyst - Gründer, Eigentümer und GF von 2 Cybersicherheitsunternehmen

- Geb. 1978 / whft. Baden bei Wien
- Leidenschaften Fußball / Geschichte
- 1999 nach Matura und BH – Eintritt in die Gendarmerie
- 1999-2024: Polizeidienst / vorwiegend operativer Kriminaldienst

- ab 2021: Gründung und Aufbau Agentur Cyberschutz / Cyber & Crime Versicherungsmakler GmbH
- Ende 2024: Beteiligungs- und Investitionsphase / Umstrukturierungen / schnell wachsend – hochspezialisiert

Agentur Cyberschutz

cyber & crime Versicherungsmakler GmbH

cybercrime Komplettschutz

cybercrime Komplettschutz INCIDENT RESPONSE SERVICE TEAM

Agentur Cyberschutz

ALLIANZ gegen Cybercrime

Zusammenschluss führender Spezialisten aus den verschiedensten Bereichen für Ihre Cybersicherheit

Agentur Cyberschutz

- **Überprüfung, Herstellung und Bestätigung** von Voraussetzungen Cyberversicherung
- **Consulting** – Aufzeigen von Möglichkeiten – 10 Kategorien / über 30 Services
- Überwachung – **externes Cyber-Risk Monitoring**

Secutec · SOPHOS Cybersecurity evolved. · HORNETSECURITY · lywand software

cyber & crime Versicherungsmakler GmbH

- umfassende **Cyber & Crime Versicherungen** + Lösegeldoption
- **Haftungs- und Deckungssicherheit**
- **KMU - Großkonzerne**

AssPro · managerline

cybercrime Komplettschutz

INCIDENT RESPONSE SERVICE TEAM

- **komplette Schadensfallbetreuung**
- in Präsenz / Remote
- Krisenstab
- IT-Forensik
- IT-Support
- Rechtshilfe
- PR-Management
- Cyber Schutzschirm
- Berichterstattung / Behördenmeldungen / Dokumentation

Agentur Cyberschutz · Secutec · tems security · ATB. LAW AZEM | TAUDES | BLOCH · mh

Agentur Cyberschutz

UNSERE QUELLEN

Unser einzigartiger Wissens- und Erfahrungsvorsprung

DARKNET-Analyse

- **weltweite Opferstatistik**
- **TÄTERPROFILE**
- **tagesaktuelle Reports**

IT-Risikoanalysen

- bis zu 400 Überprüfungen / Jahr
- Schwachstellen

Incident Reponse Service

- IT-Forensik Reports
- Angriffsverlauf
- Ausgenutzte Schwachstelle
- Gesamtschaden

cybercrime
Komplettschutz
INCIDENT RESPONSE SERVICE TEAM

Agentur Cyberschutz

Cybercrime

Attacken auf IT

Cyberattacken

- zielgerichtete Angriffe
- Unternehmen – kritische IF - Behörden
- Netzwerksicherheitsverletzungen
- Existenzbedrohende Schäden

Werkzeuge / Angriffsvektoren

- IT-Schwachstellen
- Keylogger
- DARKNET Märkte
- Admin Accounts

Ransomware / Extortion
Ransomware / Double Extortion
DDOs
Gesamtschaden: BU – IT - Daten

DARKNET

- **Kommunikations- und Handelsplattform**
- **Daten- und Schwachstellenverkauf**
- **Cybercrime as a Service - Auftragsattacken**

Social Engineering

CYBER-Betrug- und Erpressung

- Schwachstelle Mensch
- Privatpersonen / Unternehmen
- Breitgefächert / zielgerichtet

Werkzeuge / Angriffsvektoren

- Mail / Tel
- Social Engineering
- Fakemailer / Call – ID Spoofing / Fakeshops

Betrugs- und Erpressungsdelikte (12 MP):

- CEO Fraud / Fake Prs.
- Rechnungsbetrug
- Lieferumleitung
- Phishing – 148a

Agentur Cyberschutz

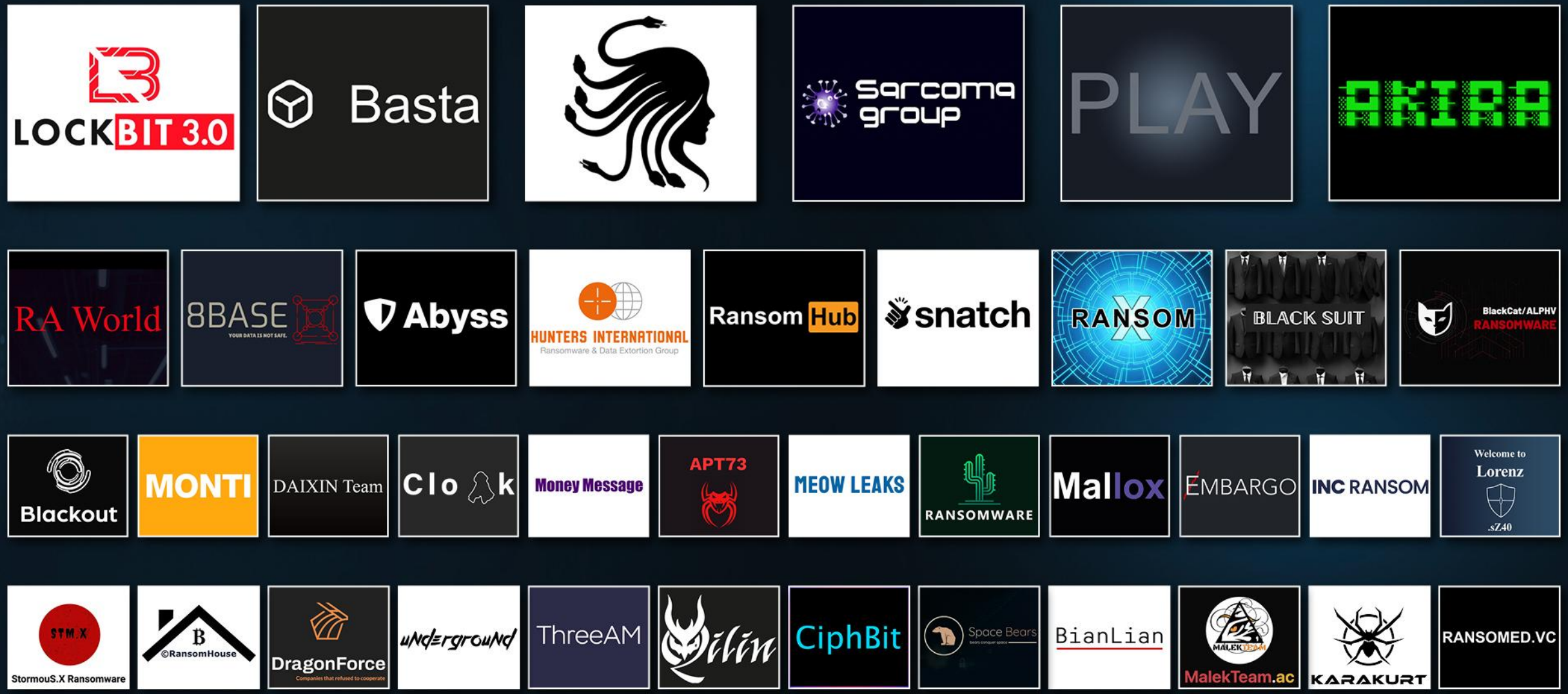
Agentur Cyberschutz Stats

- Weltweit seit 01.01.2022: 18.000 veröffentlichte Opfer mit Datenabfluss
- seit 01.01.2022 – 300 Gruppierungen
- derzeit 90 aktiv
- agieren länder- und branchenübergreifend
- identes Konzept – geringfügige Unterscheidungen

Spezifikationen – Lösegeldbemessung – Affiliate System – Vorverhandlungen

Agentur Cyberschutz

Ransomware Gangs



Agentur Cyberschutz

Gesamtkonzept Cyber- und IT-Sicherheit

Cybercrime & Solutions Unternehmensberatung

60 Min. / MS Teams

Selbstanalyse IT-Risiko

10 Knock-Outs / Gegencheck – Follow-Up Beratung

Ransomware DDoS

- Umfassend – ohne Lücken und Ausnahmen
- Gegen alle Angriffsvektoren
- Durchgehend – 24/7/52
- Automatisiert + Personaleinsatz
- Intern / extern
- Vorbereitung Schadensfall

Betrug Erpressung

Angriffsvektoren:

- VPN / Fernzugriffe
- CVE
- Keylogger
- Phishing
- M365 Account Hacking
- fehlendes Patchmanagement

Agentur Cyberschutz

Praxisbeispiel

E-Mail-Account-Compromise (EAC)

- Massenphänomen seit Juni 2025
- M365 oder Mail Programm kompromittiert
- 2 Szenarien: Fake Rechnungen oder Link zu Schadsoftware
- gegenwärtig 7/10 Schadensfälle EAC – 3/10 Ransomware Double Extortion

Agentur Cyberschutz

Praxisbeispiel

E-Mail-Account-Compromise (EAC)

Opfer: Reifenhändler in NÖ / 7 Clients / 3 Mio. Umsatz / 1.500 Kunden

Versicherungskunde: 1 Mio. VS

IT-Security:

- unterschwelliger Virenschutz
- kein secureDNS
- kein Darknet-Monitoring
- kein Mail-Protection Paket

Agentur Cyberschutz

Timeline / Angriffsablauf – Verständigungen – Berichte

April 2025

- **07.04.** Vorbereitungshandlungen der Täter – System kompromittiert / WebDAV-Share mit Programmiersoftware Python infiziert

August 2025

- **14.08.** Fake-Mail Versand an 1.453 Empfänger über die office Adresse
- **14.08.** Betroffene melden sich per Mail und telefonisch / Link wurde geöffnet
- **14.08.** IT-Support / Erstanalyse
- **14.08.** Start IT-Forensik vor Ort
- **14.08.** Darknet Monitoring aktiviert – 1 Plain-Text Treffer office Adresse aus 2021
- **14.08.** XDR ausgerollt
- **14.08.** Benachrichtigung der Betroffenen / Warnung – Anleitungen
- **16.08.** Polizeianzeige - Erstanzeige
- **16.08.** Versand DSGVO Erstmeldung / Einstellung noch offen
- **16.08.-24.08.** Beantwortung zahlreicher Auskunftsbegehren und Rückmeldungen von Betroffenen
- **27.08.** IT-Forensik Endreport

Oktober 2025

- **20.10.** Nachtrags- Abschlussmeldung Anzeige Polizei
- **20.10.** Nach- und Hochrüsten / Darknet Monitoring – XDR – secureDNS – CVE intern / extern / MFA / **Hornet Plan 4**
- **20.10.** Endbericht an Versicherer / keine Regressforderungen

Agentur Cyberschutz

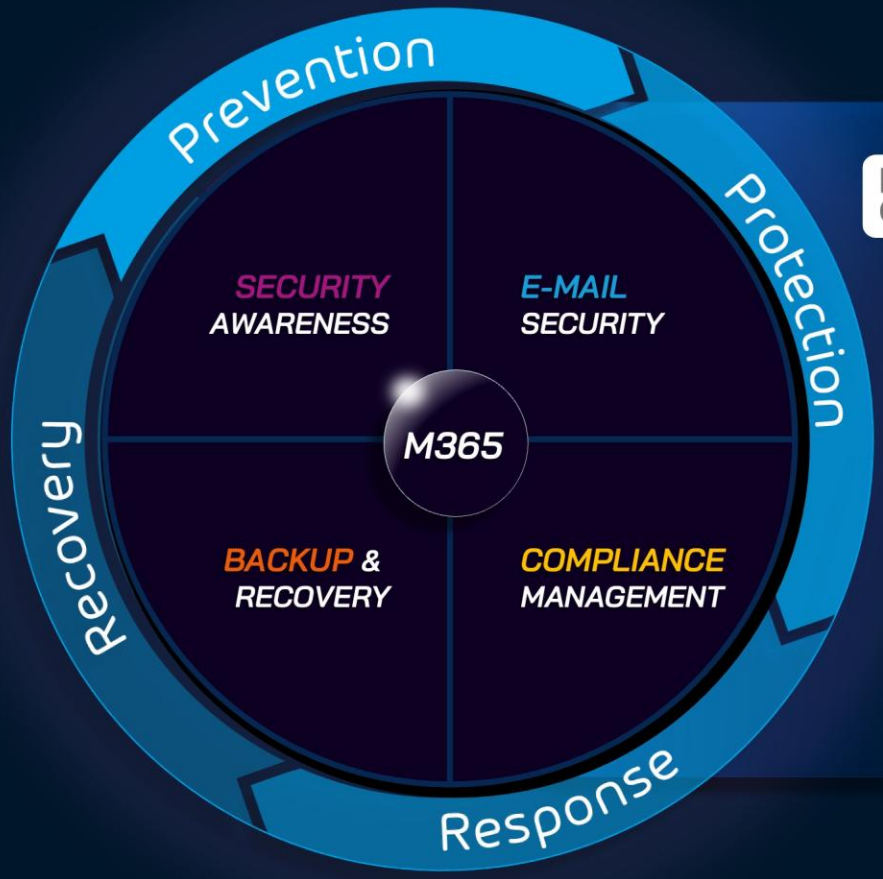
HORNETSECURITY WHAT WE ARE

MARKUS TODT
Country Manager, AT

HORNETSECURITY

HORNETSECURITY WHAT WE ARE

CYBER TRUST AUSTRIA



BMW GROUP · MINI · ROLLS-ROYCE MOTOR CARS LTD · GLOBUS

KUKA · LVM VERSICHERUNG · KONICA MINOLTA

CLAAS · PORSCHE HOLDING

Bayerisches Rotes Kreuz · OTTO

HORNETSECURITY

HORNETSECURITY SECURITY LAB

Security Lab mit globaler Threat Intelligence

5.4 Milliarden analysierte E-Mails pro Monat

60+

Mitarbeiter weltweit

Team aus internationalen IT-Security Spezialisten

24/7

Monitoring von Erkennungs-mechanismen

Monthly Threat Report & Security Trends

HORNETSECURITY WORKSHOP

SECURITY AWARENESS SERVICE

15:05 – 15:50 Uhr

Cyberkriminelle schlafen nicht – auch nicht in Österreich – wie Sie Ihre Belegschaft mit lokal ausgerichteter Awareness wirklich stärken

PHISHING BLEIBT GRÖßTER RISIKOFAKTOR

95%

aller Cyber-Attacken starten mit einer E-Mail

91%

aller Cybersicherheitsvorfälle sind auf menschliches Fehlverhalten zurückzuführen

HORNETSECURITY