

TAR•X

CYBER SECURITY

Ganzheitlicher Schutz vor
Cyberattacken



„Bei der TAROX Security setzen wir unser Vertrauen stets auf moderne Techniken und gesunden Menschenverstand. Die Kombination aus beidem ermöglicht uns den bestmöglichen Schutz.“

Alexander Wiediker, Head of Cyber Security

INHALT

Einleitung	04	TAROX DNS-Shop	25
Ganzheitlicher Schutz	06	SIEM Das Frühwarnsystem	26
NIS-2 Compliance	08	Security Awareness	28
Ansprechpartner	10	Netzwerksicherheit	30
Cyberbedrohungen im Wandel	14	Firewall als Grundlage	32
Penetrationstest	16	Unsere Partner	34
Endpoint Security	18		
Schwachstellenmanagement	20		
Passwortmanagement	22		
SystoLOCK Passwortlose MFA	24		





TAROX CYBER SECURITY – ZUKUNFTSWEISENDE CYBER- SICHERHEITSLÖSUNGEN

Die TAROX Cyber Security berät Sie individuell und bietet Ihnen die auf die Bedürfnisse Ihrer Kunden angepassten Lösungen. Sowohl bei der Inbetriebnahme aber auch bei komplizierten Konfigurationen nimmt Sie das kompetente Team gerne an die Hand und überzeugt darüber hinaus mit einem umfangreichen Schulungsangebot nach Best Practice.



TAROX



ALEXANDER WIEDIKER HEAD OF CYBER SECURITY

„Wir unterstützen Sie bei IT-Sicherheit und Datenschutz und setzen gemeinsam mit Ihnen passende Maßnahmen für Ihr Unternehmen um.“

 alexander.wiediker@tarox.de

 +49 231 98980-312

ERFAHREN SIE
MEHR ÜBER UNS



GANZHEITLICHER SCHUTZ vor Cyberattacken

Wir beraten Sie kompetent und unterstützen Sie bei der Implementierung.

ERFAHREN SIE
MEHR ÜBER UNS



UNSERE EXPERTISE FÜR MODERNE IT-SICHERHEIT

Unser Team vereint tiefgehende technische Expertise mit aktueller regulatorischer Kompetenz. Wir arbeiten konsequent nach den Vorgaben und Empfehlungen des BSI und stellen sicher, dass unsere Lösungen sowohl technisch als auch gesetzlich auf dem neuesten Stand sind.

Ein zentraler Bestandteil unseres Ansatzes sind enge technologische Partnerschaften mit führenden Security-Herstellern. Gemeinsam entwickeln wir passgenaue Sicherheitslösungen, die sich an realen Anforderungen orientieren. Dabei ist es uns wichtig, Cyber Security verständlich, transparent und auf Augenhöhe zu vermitteln – und ein komplexes Thema pragmatisch und lösungsorientiert anzugehen.



TAROX – IHR IDEALER PARTNER für NIS-2-Compliance



Abfall



Abwasser



Anbieter
digitaler Dienste



Banken



Digitale
Infrastruktur



Energie



Ernährung



Finanzmarkt-
infrastruktur



Forschung



Gesundheit



Industrie



Gefährliche
Chemikalien



Post



Transport



Trinkwasser



Verwaltung



Verwaltung von
IKT-Diensten



Weltraum





DIE NIS-2-RICHTLINIE STELLT HÖHERE ANFORDERUNGEN AN IT-SICHERHEIT IN EUROPA – SOWOHL TECHNISCH ALS AUCH ORGANISATORISCH.

Wir unterstützen Sie mit passenden Leistungen in Bereichen wie Sicherheitslösungen, Monitoring, Zugriffsschutz, Datenschutz und Beratung bei der Umsetzung dieser Anforderungen.

Kurz gesagt:

Wir begleiten Sie von der Risikoanalyse bis zum laufenden Betrieb und helfen Ihnen, die Anforderungen von NIS-2 strukturiert und zuverlässig umzusetzen.

CYBERSICHERHEIT FÜR KMU: STRUKTURIERT & EFFEKTIV

Das BSI empfiehlt kleinen und mittleren Unternehmen (KMU), ihre Cybersicherheit strukturiert und risikoorientiert anzugehen. Ziel ist es, mit überschaubarem Aufwand ein angemessenes Sicherheitsniveau zu erreichen.

Wichtige Maßnahmen sind:

- IT-Sicherheit im Unternehmen klar organisieren
- Grundlegende technische Schutzmaßnahmen umsetzen
- Zugriffe und Benutzerkonten absichern
- Regelmäßige Datensicherungen und Notfallpläne einrichten
- Mitarbeitende für Sicherheitsrisiken sensibilisieren
- Sicherheitsmaßnahmen regelmäßig überprüfen



ANSPRECH- PARTNER

LUCAS HEYMANN
PRODUCT MANAGER
CYBER SECURITY

✉ lucas.heymanntarox.de

☎ +49 231 98980-665



10

Cyber Security



**ATILLA CAMCI
CONSULTANT
CYBER SECURITY**

 service.security@tarox.de

 +49 231 98980-665



**SIMON MAY
CONSULTANT
CYBER SECURITY**

 service.security@tarox.de

 +49 231 98980-665



11

**ROUVEN SCOBEL
TEAMLEAD SALES
CYBER SECURITY**

 rouven.scobel@tarox.de

 +49 231 98980-316



**THOMAS PABST
SENIOR SALES CONSULTANT
CYBER SECURITY**

 thomas.pabst@tarox.de

 +49 231 98980-315



Cyber Security



TIM FISCHER
SALES CONSULTANT
CYBER SECURITY

 tim.fischer@tarox.de

 +49 231 98980-323



OLIVER GOETHE
SALES CONSULTANT
CYBER SECURITY

 oliver.goethe@tarox.de

 +49 231 98980-318



13

Cyberbedrohungen im Wandel – Sicherheit muss mithalten

Die Zeit von Antivirus und klassischen Firewalls ist längst vorbei. Durch frei verfügbare KI hat sich das Wettrüsten zwischen Cyberkriminellen und Unternehmen deutlich verschärft. Moderne KI-gestützte Erkennung, automatisiertes Schwachstellenmanagement und geschulte Mitarbeiter-Awareness sind heute zentrale Bausteine für umfassenden Unternehmensschutz.



PAIN POINTS

HOHER BETRIEBS- UND WARTUNGSAUFWAND

Antivirus-, Firewall- und EDR-Lösungen erfordern laufende Pflege wie Updates und Policy-Anpassungen. Dieser Aufwand skaliert schlecht und ist oft nicht vollständig abgedeckt.

FEHLENDE TRANSPARENZ IM SCHWACHSTELLENMANAGEMENT

Oft fehlt ein strukturiertes Vulnerability Management. Unvollständige Scans und fehlende Priorisierung verringern die Wirksamkeit von Maßnahmen.

SCHWIERIGE MONETARISIERUNG VON SICHERHEITSANALYSEN

Pentests und Assessments sind erklärungsbedürftig und aus Kundensicht oft kostenintensiv. Der Mehrwert lässt sich schwer vermitteln und integrieren.

MENSCHLICHER FAKTOR ALS SICHERHEITSRISIKO

Schwache Passwörter und geringe MFA-Nutzung unterlaufen Schutzmaßnahmen. Der Einfluss auf Nutzerverhalten ist begrenzt.

14

MODERNE LÖSUNGEN FÜR IT-SICHERHEIT



ZENTRALISIERTE SECURITY-PLATTFORM

Unsere Lösungen bündeln Antivirus, Firewall und Endpoint-Security in einer Plattform. Einheitliche Policies, automatisierte Updates und Mandantenfähigkeit reduzieren den Aufwand und ermöglichen skalierbare Services.



INTEGRIERTES SCHWACHSTELLENMANAGEMENT

Kontinuierliche Scans und Risikobewertungen priorisieren Schwachstellen. Klare Empfehlungen und Reports unterstützen ein strukturiertes Management.



STANDARDISIERTE SECURITY-ASSESSMENTS

Pentests und Sicherheitsprüfungen lassen sich als wiederholbare Services anbieten. Das erhöht die Skalierbarkeit und erleichtert die Integration in Service- und Compliance-Modelle.



TECHNISCHE DURCHSETZUNG SICHERER NUTZERPRAKTIKEN

Passwortregeln, MFA und automatisierte Policies reduzieren Risiken durch Nutzerverhalten und setzen Sicherheitsvorgaben konsequent um.

15

AUTOMATISIERTE PENETRATIONSTESTS

Für den ultimativen Schutz: Effiziente Sicherheitsprüfung Ihres Unternehmens auf Knopfdruck.

Automatisierte Pentests mit unserem Partner Enginsight

Schützen Sie Ihr Unternehmen mit einer Lösung, die wie ein Hacker denkt – aber auf Ihrer Seite steht. Schwachstellen werden frühzeitig erkannt und Ihre IT nachhaltig abgesichert.

Maximale Sicherheit – minimaler Aufwand

Ihre Systeme werden automatisiert und rund um die Uhr getestet. Die Plattform erkennt Sicherheitslücken, bewertet Risiken und liefert klare Handlungsempfehlungen – alles in einer zentralen Lösung.

- Schritt 1: IT-Inventarisierung
- Schritt 2: IT-Security-Analyse von innen
- Schritt 3: IT-Security-Analyse von außen
- Schritt 4: Security-Prozesse automatisieren
- Schritt 5: Automatischer Penetrationstest





HACKER-PERSPEKTIVE INKLUSIVE

Simulierte Angriffe aus interner und externer Sicht mit vollständigem Footprinting und automatischer Analyse aller erreichbaren Systeme.

CVE-SCANNER AUF ENTERPRISE-NIVEAU

Erkennt relevante Software-Schwachstellen und kann optional mit Zugangsdaten für tiefere Analysen erweitert werden.

PASSWORT-CHECK PER BRUTEFORCE

Identifiziert schwache oder kompromittierte Passwörter und unterstützt gängige Dienste wie SSH, RDP, SQL oder FTP.

SERVICE-CHECKS UND FEHLKONFIGURATIONEN

Prüft zentrale Dienste wie SSL/TLS, DNS, LDAP oder SMTP und erkennt gefährliche Fehlkonfigurationen. Erweiterbar durch eigene Pentest-Skripte (z. B. Python oder Bash).

TRANSPARENTE ERGEBNISSE

Auditberichte, automatisierte Risikoanalysen und priorisierte Maßnahmen – inklusive Vergleich zu früheren Tests.

KONTINUIERLICHER SICHERHEITSPROZESS

Pentesting wird zum regelmäßigen, automatisierten Prozess mit wiederkehrenden Prüfungen und langfristiger Verbesserung der IT-Sicherheit.



ULTIMATIVER SCHUTZ – die nächste Generation der Endpoint Security



**TAROX CYBER SECURITY BIETET EIN UMFASSENDES SCHUTZKONZEPT FÜR UNTERNEHMEN –
VON DER ERKENNUNG BIS ZUR ABWEHR MODERNER CYBERBEDROHUNGEN**

Im Fokus stehen drei zentrale Technologien:

XDR – Plattformübergreifende Echtzeit-Erkennung und automatische Reaktion auf Bedrohungen durch Analyse von Endpoints, Netzwerk und Cloud.

MDR – 24/7-Überwachung durch ein Security Operations Center kombiniert mit moderner Technologie – für maximale Sicherheit ohne eigenes Security-Team.

ZTNA – Moderne Zugriffskontrolle nach dem Zero-Trust-Prinzip als sichere Alternative zu klassischen VPNs.

18

ERFAHRUNG, DIE SCHÜTZT

Mit über 30 Jahren IT-Erfahrung bringen die TAROX Cyber Security Consultants Expertenwissen aus Vertrieb, Projektgeschäft, Datenschutz und Herstellersystemen direkt in Ihre Sicherheitsstrategie ein.

IHRE SECURITY VERDIENT DAS BESTE – WIR BERATEN SIE GERNE

Egal ob Sie Ihre IT modernisieren, Angriffe verhindern oder Ihre Sicherheitsstrategie neu aufstellen möchten:

Unsere Spezialisten entwickeln die perfekte Lösung für Ihr Unternehmen.

Cyber Security



CYBER SECURITY MIT STARKEN PARTNERN

TAROX arbeitet mit führenden Herstellern zusammen, um jede Sicherheitsanforderung passgenau abzudecken:

- **SOPHOS MSP FLEX** – flexible, nutzungsbasierte Endpoint Security
- **SOPHOS SUBSCRIPTIONS** – kalkulierbarer Rundumschutz
- **BITDEFENDER MSP** – mandantenfähige Enterprise-Technologie
- **BITDEFENDER SUBSCRIPTIONS** – KI-Schutz für jedes Unternehmen
- **SECUREPOINT ANTIVIRUS** – Made in Germany, Made for Security

19

SCHWACHSTELLEN- MANAGEMENT:

Behalten Sie die Schwachpunkte Ihrer Technik ständig im Überblick, um proaktiv auf diese reagieren zu können



IDENTIFIKATION

- Automatisierte Sicherheitsscans erkennen potenzielle Schwachstellen im gesamten System, basierend auf vorhandenen Datenbanken und dem Software-Inventar. So wird sichergestellt, dass alle relevanten Sicherheitslücken erfasst werden.

20

BEWERTUNG

→ Jede gefundene Schwachstelle wird hinsichtlich ihrer Kritikalität und ihres Risikos bewertet. Dadurch lassen sich Prioritäten setzen und besonders gefährliche Lücken gezielt zuerst beheben.

Cyber Security



BEHEBUNG

→ Identifizierte Schwachstellen werden durch Patches, Updates oder Konfigurationsanpassungen geschlossen. Das System liefert konkrete Handlungsempfehlungen und zeigt auf, wie Angreifer die Lücke ausnutzen könnten. Wenn kein Patch verfügbar ist, können Maßnahmen getroffen werden, um die Schwachstelle zu verstecken oder abzumildern.

21

ULTIMATIVES PASSWORT- MANAGEMENT FÜR EXPERTEN – Sicherheit auf höchstem Niveau

Ein moderner Passwortmanager bietet nicht nur sicheren Schutz für Zugangsdaten, sondern erleichtert zugleich den digitalen Alltag.

Durch intelligente Funktionen wie Synchronisierung, Mehrfaktorsicherheit, Single Sign-On und automatische Formularausfüllung wird der Zugriff auf Anwendungen schneller, komfortabler und deutlich sicherer.

22



SYNCHRONISIERUNG
ÜBER ALLE GERÄTE

Ein Passwortmanager sollte Passwörter und gespeicherte Daten automatisch auf allen Geräten synchronisieren, damit Nutzer jederzeit und überall Zugriff auf ihre Konten haben.



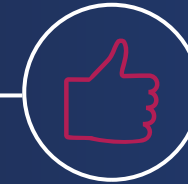
MULTI-FAKTOR-
AUTHENTIFIZIERUNG
(MFA)

Zur Erhöhung der Sicherheit sollte neben dem Passwort ein zweiter Faktor nutzbar sein – z. B. Fingerabdruck, App-Bestätigung oder Einmalpasswort.



SINGLE SIGN-ON
(SSO)

Durch die Kombination von SSO und Passwortmanager lässt sich die Anzahl benötigter Passwörter reduzieren. Gleichzeitig wird der Zugriff auf Anwendungen erleichtert und zentral kontrolliert



AUTOMATISCHES
AUSFÜLLEN

Der Passwortmanager sollte Anmeldeformulare automatisch mit Benutzernamen und Passwort befüllen, um Zeit zu sparen und Fehler zu vermeiden.

PASSWORTLOSE MFA – Schutz für Ihr Unternehmen

Mit unseren Lösungspartnern bieten wir eine passwortlose MFA-Lösung zum Schutz vor Phishing und Identitätsangriffen bei allen Logins.

Zero-Trust beginnt bei der Anmeldung – ohne Passwörter, ohne Lücken

Phishing- und Social-Engineering-Angriffe werden immer raffinierter: über 60 % der Unternehmen sind regelmäßig betroffen. Viele MFA-Methoden reichen nicht mehr aus. Phishingresistente, passwortlose Lösungen bieten hier eine sichere und benutzerfreundliche Alternative für On-Premises- und Cloud-Identitäten.

Regulatorisch konforme MFA – integriert in alle Zugriffsszenarien:

- Windows-Anmeldung
- RDP-Anmeldung
- Anmeldung bei VPN
- Privilegienerhöhung
- Identitätswechsel
- Offline-Anmeldung
- Anmeldung bei Office 365
- Anmeldung bei externen Ressourcen

Dabei erfüllen wir NIS2, DORA und PCI DSS und schützen umfassend vor identitätsbasierten Cyberbedrohungen.

24

TAROX DNS-SHOP – Domains und Zertifikate einfach verwalten

Domains und digitale Zertifikate sind eine zentrale Grundlage für den sicheren und professionellen Betrieb von Online-Diensten. Sie ermöglichen eine eindeutige Erreichbarkeit im Internet und sorgen durch Verschlüsselungstechnologien wie TLS/SSL, S/MIME oder Code Signing für geschützte Kommunikation und Vertrauen.

Mit dem TAROX DNS-Shop bieten wir Ihnen eine zentrale Plattform für Domains, DNS und digitale Zertifikate:

- Einfache Registrierung und Verwaltung von Domains und DNS-Einträgen
- Zugriff auf über 1.000 Domain-Endungen
- Verfügbarkeit von Zertifikaten führender Anbieter wie DigiCert, GeoTrust und GlobalSign
- Geeignet für den Aufbau oder die Erweiterung Ihres Reseller-Geschäfts

25

SECURITY INFORMATION AND EVENT MANAGEMENT – das Frühwarnsystem

„In Kombination mit der TAROX Security wird ein SIEM-System zu einem leistungsstarken Werkzeug, das Unternehmen ganzheitlich schützt, Transparenz schafft und eine robuste Grundlage für langfristige Cyber-Resilienz bildet.“



ARCHIVIERUNG UND DATENVERWALTUNG – ALLES SAUBER DOKUMENTIERT

SIEM-Systeme speichern Protokolle und Ereignisse zentral ab.

Diese Daten werden für Compliance, Audits und forensische Analysen aufbewahrt, damit Vorfälle später nachvollzogen und gesetzliche Anforderungen erfüllt werden können.

ECHTZEITANALYSE – BEDROHUNGEN SOFORT ERKENNEN

Dank Echtzeitüberwachung erkennen SIEM-Systeme Sicherheitsvorfälle im Moment ihres Entstehens.

Auffälliges Verhalten wird sofort analysiert und es werden unmittelbar Warnungen ausgegeben – bevor ein größerer Schaden entsteht.

FORENSIK – VORFÄLLE NACHVOLLZIEHEN & VERSTEHEN

Nach einem Sicherheitsvorfall helfen SIEM-Systeme dabei, den Ablauf genau zu rekonstruieren:

Was ist passiert? Wie konnte es passieren? Welche Systeme sind betroffen? So lassen sich Sicherheitslücken schließen und zukünftige Angriffe verhindern.

FAZIT ←

SIEM-Systeme sind ein zentraler Baustein moderner Cyber Security. Genau hier setzt **TAROX Security** mit einem ganzheitlichen Ansatz an: Unternehmen erkennen, bewerten und beheben Risiken frühzeitig – durch die Kombination von XDR, MDR, Zero-Trust-Konzepten sowie integrierten Daten- und Datenschutzstrategien.

SICHERHEIT BEGINNT MIT BEWUSSTSEIN – Gemeinsam gegen Cyberbedrohungen

Der Mensch entscheidet über Sicherheit

Cyberangriffe beginnen selten mit Technik – sondern mit einem Klick. Phishing, Social Engineering und unsichere Passwörter gehören zu den häufigsten Ursachen erfolgreicher Sicherheitsvorfälle. Trotz moderner IT-Schutzmaßnahmen bleibt der menschliche Faktor das größte Risiko – und zugleich die größte Chance.

WARUM SECURITY AWARENESS?

- Über 80 % aller Cyberangriffe nutzen menschliche Fehlentscheidungen
- Phishing-E-Mails werden immer professioneller
- Ein einzelner Klick kann gravierende Folgen haben
- Compliance-Anforderungen steigen kontinuierlich (z. B. ISO 27001, NIS2)

28



UNSER ANSATZ

- Security Awareness macht Mitarbeitende handlungssicher
- Erkennen von Phishing- und Social-Engineering-Angriffen
- Sicherer Umgang mit E-Mails, Passwörtern und Daten
- Praxisnahe Sensibilisierung statt theoretischer Schulung
- Nachhaltige Stärkung der Sicherheitskultur

IHR MEHRWERT

- Reduzierte Sicherheitsvorfälle
- Geringeres Haftungs- und Compliance-Risiko
- Gestärktes Sicherheitsbewusstsein im Unternehmen
- Mitarbeitende als „Human Firewall“

**SECURITY AWARENESS IST KEINE OPTION –
sie ist ein zentraler Bestandteil moderner
IT-Sicherheit.**

NETZWERKSICHERHEIT

Ganzheitliche Sicherheit für eine widerstandsfähige und zukunftsfähige IT-Infrastruktur.

Angesichts zunehmender digitaler Bedrohungen ist der Schutz der IT-Infrastruktur für Unternehmen wichtig. Firewalls bilden dabei die Grundlage, indem sie unerwünschte Zugriffe verhindern und Daten schützen.

Ergänzende Maßnahmen wie Bedrohungserkennung, Verschlüsselung und Cloud-Absicherung erweitern diesen Schutz. Zusammen sorgen sie für eine zuverlässige und sichere IT-Umgebung.





NEXT-GENERATION FIREWALL (NGFW)

Moderne Firewall mit Funktionen wie IDS/IPS und Anwendungssteuerung zum Schutz vor Bedrohungen und zur Steuerung des Datenverkehrs.

SSL/TLS-ENTSCHLÜSSELUNG

Ermöglicht die Prüfung verschlüsselter Verbindungen zur frühzeitigen Erkennung von Bedrohungen unter Berücksichtigung des Datenschutzes.

INHALTSBASIERTE BEDROHUNGSERKENNUNG

Stellt sichere, verschlüsselte Verbindungen für Standorte und Remote-Zugriffe bereit.

NETZWERKSEGMENTIERUNG

Teilt das Netzwerk in Bereiche auf, um Risiken zu reduzieren und sensible Systeme zu schützen.

CLOUD-SICHERHEIT

Schützt Anwendungen und Daten in der Cloud und unterstützt eine sichere Nutzung.

AUTOMATISIERUNG UND ORCHESTRIERUNG

Unterstützt schnellere Reaktionen durch automatisierte Abläufe und abgestimmte Sicherheitstools.

SKALIERBARKEIT, EINFACHE VERWALTUNG UND COMPLIANCE

Flexibel erweiterbar, zentral verwaltbar und hilfreich bei der Einhaltung von Sicherheitsanforderungen.

FIREWALLS ALS GRUNDLAGE MODERNER IT-SICHERHEIT

Eine moderne Firewall ist ein zentrales Element der IT-Sicherheit. Sie schützt Unternehmen vor externen Zugriffen, hilft beim Schutz sensibler Daten und unterstützt bei der Einhaltung rechtlicher Vorgaben.

Die folgenden Kernbereiche zeigen, welche Aufgaben eine Firewall dabei übernimmt:

→ NETZWERKSICHERHEIT

Eine Firewall bildet die Schnittstelle zwischen internem Netzwerk und externen Verbindungen. Sie überwacht den Datenverkehr und blockiert unbefugte Zugriffe sowie schädliche Inhalte.

So werden typische Bedrohungen wie Malware oder Angriffe aus dem Internet abgewehrt.

32

→ DATENSCHUTZ

Durch gezielte Firewall-Regeln lässt sich genau steuern, wer auf welche Daten zugreifen darf.

Dies verhindert Datenlecks, schützt vertrauliche Informationen und stellt sicher, dass sensible Daten ausschließlich berechtigten Personen zugänglich sind.

→ COMPLIANCE-EINHALTUNG

Eine Firewall trägt maßgeblich dazu bei, gesetzliche Vorgaben und branchenspezifische Sicherheitsstandards einzuhalten. Sie sorgt dafür, dass Sicherheitsrichtlinien konsequent umgesetzt werden und erleichtert gleichzeitig interne wie externe Audits.

Dadurch sinken rechtliche Risiken und potenzielle Bußgelder, während das Vertrauen von Kunden und Partnern nachhaltig gestärkt wird.





UNSERE PARTNER



35

