



# **CYBERRESILIENZ**

**EXPLORE WITH US!**

*netlogix | Ihr IT-Dienstleister aus Nürnberg.*

■ IT-SERVICES ■ IT-TRAINING ■ WEB SOLUTIONS ■ NLX.CLOUD

# WAS IST

# CYBERRESILIENZ?

*Willkommen bei netlogix, Ihrem sympathischen Partner im Bereich Cyberresilienz.*

*Die digitale Welt ist von Bedrohungen geprägt. Für Unternehmen sind daher drei Dinge wichtig: auf Angriffe vorbereitet zu sein, sich im Ernstfall schnell zu erholen und gestärkt aus Vorfällen hervorzugehen. Genau hier kommt das Konzept der Cyberresilienz ins Spiel.*

*Cyberresilienz ist die Fähigkeit eines Unternehmens, Cyberangriffe zu antizipieren, ihnen entgegenzuwirken und sich von ihnen zu erholen.*

*Es geht darum, nicht nur die Technologie zu schützen, sondern auch die Prozesse, Menschen und den gesamten Betriebsablauf widerstandsfähiger gegenüber den immer raffinierteren Angriffsmethoden zu machen.*

**CYBERRESILIENZ IST WIE EIN ROBUSTES NETZ, DAS IM FALLE EINES ANGRIFFS NICHT REISST, SONDERN DEN STOSS ABSORBIERT UND DIE ORGANISATION SCHNELL WIEDER AUF DIE BEINE BRINGT.**

# UNSERE HERANGEHENSWEISE

**B**ei netlogix verstehen wir, dass Cyberresilienz kein Einheitskonzept ist. Jedes Unternehmen hat einzigartige Bedürfnisse und Risikoprofile. Deshalb arbeiten wir eng mit unseren Kunden zusammen, um individuell zugeschnittene Cyberresilienz-Strategien zu entwickeln. Wir bieten nicht nur modernste Technologien zur Erkennung und Abwehr von Bedrohungen, sondern legen auch großen Wert auf pro-aktives Training und Awareness, um Ihre Mitarbeiter zu befähigen, potenzielle Risiken zu erkennen.

**U**nseren Experten verfolgen einen ganzheitlichen Ansatz, der sowohl präventive Maßnahmen als auch reaktive Strategien einschließt. Von der Sicherung Ihrer Netzwerke und Daten über das Erstellen von Disaster Recovery und Backup Plänen bis zur kontinuierlichen Überwachung und Analyse – wir sind Ihr Partner für umfassende Cyberresilienz.

## *Warum netlogix?*

**D**ie langjährige Erfahrung und unser tiefes Verständnis für die sich ständig ändernde Bedrohungslandschaft versetzen uns in die Lage, maßgeschneiderte Lösungen zu liefern, die Ihre Organisation widerstandsfähig und agil halten. Mit uns an Ihrer Seite können Sie sicher sein, dass Sie nicht nur auf Angriffe vorbereitet sind, sondern auch die Fähigkeit besitzen, sich schnell zu erholen und gestärkt daraus hervorzugehen.

# DER WEG ZUR CYBERRESILIENZ

## 1. ENDPOINT SECURITY

Hochmoderne Endpoint Security für ultimativen Schutz.

## 4. SECURE APPLICATION DELIVERY

Maximale Performance und Sicherheit für Ihre Anwendungen.

## 2. MANAGED DETECTION AND RESPONSE

Sorgenfrei durch aktive Cybersecurity Operations.

## 5. E-MAIL-SICHERHEIT UND VERSCHLÜSSELUNG

Gesicherte Kommunikation mit der Außenwelt.

## 3. FIREWALL

Sichere Vernetzung in einer vernetzten Welt.

## 6. AUTHENTIFIZIERUNG UND PASSWORTMANAGEMENT

Schützen Sie Ihre Identität.

## 8. SWITCHING

Leistungsstarke Netzwerkinfrastruktur für die moderne Unternehmenswelt

## 9. IT-SEC-CHECK

Gewissheit über den Zustand Ihrer IT und Ihrer IT-Sicherheit.

**SIE SIND NUN  
CYBERRESILIENT!**

## 12. IT-TRAINING

Komplettes Angebot an Seminaren, Workshops und individuellen Trainings mit vielen weiteren Serviceleistungen.

## 10. RANSOMWARE PROTECTION

Erkennung von verdächtigem Ransomware-Verhalten, bevor Angreifer die Kontrolle über Ihre Daten erhalten.

## 11. SUPA

Sensibilisieren Sie Ihre Mitarbeiter für digitale Bedrohungen und schützen Sie so Ihre Daten.

## 7. WIFI

Sicherer und zuverlässiger WLAN-Zugang

# KOMPONENTEN AUS UNSEREM PORTFOLIO



## 1. ENDPOINT SECURITY

Endpoint Security ist mehr als nur Virenschutz. Mit diesem wichtigen Bestandteil jeder Sicherheitsstrategie schützen Sie Endpoints, mobile Endgeräte, E-Mails und Netzwerkzugänge vor Malware, Spam sowie Datenverlusten und sichern Unternehmensdaten durch Verschlüsselung. Eine Verbindung zur Firewall regelt abhängig vom Compliance-Zustand den Zugriff auf Unternehmensdaten. Wir unterstützen Sie dabei, die optimale Endpoint-Security-Lösung zu finden und sorgen dafür, dass Sie bei Technologien wie Managed Threat Response, Behaviour Analysis und Deep Learning den Überblick behalten.



## 2. MANAGED DETECTION & RESPONSE

Rund um die Uhr aktive Cybersecurity Operations sind für Unternehmen mittlerweile zwingend notwendig. Moderne Betriebsumgebungen sind jedoch hochkomplex und Cyberbedrohungen entwickeln sich permanent weiter. Das macht es Unternehmen zunehmend schwer, sich komplett selbst um das Erkennen und Bekämpfen von Cyberbedrohungen zu kümmern.

Mit MDR stoppen unsere Experten für Sie komplexe, manuell gesteuerte Angriffe. Wir beseitigen Bedrohungen, bevor diese Ihre Geschäftsabläufe stören oder sensible Daten gefährden können.





### 3. FIREWALL

Die geschützte Vernetzung von Standorten und die Absicherung von Netzwerken sind essenzielle Anforderungen im täglichen IT-Geschäft. Durch die Verlagerung der Arbeit ins Homeoffice erweitert sich die potenzielle Angriffsfläche physikalisch um ein Vielfaches. Wir betrachten in unseren Firewallkonzepten bedingte Zugriffsmechanismen wie ZTNA (Zero Trust Network Access) sowie hochverfügbares Uplink Management (SD-WAN) und erarbeiten für Sie die passende Lösung.



### 4. SECURE APPLICATION DELIVERY

Unsere Lösungen für die Anwendungsbereitstellung sind dafür konzipiert, Performance und Sicherheit geschäftskritischer Anwendungen zu gewährleisten. Die Lösungen basieren auf einem umfassenden Application Delivery Controller und erweiterter WAN-Funktionalität und sorgen dank optimiertem Benutzerkomfort für einen erfolgreichen Geschäftsbetrieb.



# KOMPONENTEN AUS UNSEREM PORTFOLIO



## 5. E-MAIL-SICHERHEIT UND VERSCHLÜSSELUNG

E-Mails sind ein wichtiges Werkzeug für die tägliche geschäftliche Kommunikation und Produktivität. Sie sind auch ein beliebter Angriffsvektor bei sogenannten Threat Actors, die versuchen, Anmeldeinformationen zu stehlen, sensible Daten zu erhalten oder diese für Lösegeld zurückzuhalten beziehungsweise über den Zugang zu Bankinformationen Geld zu stehlen. Da Angreifer immer anspruchsvollere Multi-Vektor-Kampagnen gegen ihre Ziele einsetzen, muss E-Mail-Sicherheit mehrstufigen Schutz bieten. Unser Lösungsportfolio schützt vor dem gesamten Spektrum von Bedrohungen.



## 6. AUTHENTIFIZIERUNG UND PASSWORTMANAGEMENT

Eine konsequente Sicherheitsstrategie kommt um eine starke Authentifizierung als zusätzliche Sicherheitsschicht nicht herum. Mit unseren Mehr-Faktor-Authentifizierungslösungen sowie einem smarten Passwortmanagement für Unternehmen sichern wir die Basis für 90% aller Eintrittsvektoren: den User.





## 7. WIFI

Der komfortable, mobile Zugriff auf das Internet oder Firmennetz ist wichtig – oberste Kriterien dabei: Sicherheit und Verfügbarkeit. Mit unserer Beratung erhalten Sie eine stabile WLAN-Lösung mit höchster Ausfallsicherheit, geeignet für Netzwerke jeder Art.



## 8. SWITCHING

Eine moderne Netzwerkinfrastruktur verknüpft alle Standorte eines Unternehmens und bietet schnellen und sicheren Zugriff auf Anwendungen. Durch die zunehmende Anzahl an Applikationen steigt das Volumen der übertragenen Informationen kontinuierlich. Gleichzeitig erwarten Benutzer eine zuverlässige Performance und höchsten Schutz zu jedem Zeitpunkt. Unsere Experten beraten Sie anhand der bestehenden Umgebung, um die Anforderungen an Ihr zukünftiges Netzwerk zu erfüllen und unterstützen Sie bei der Implementierung sowie der nachhaltigen Betreuung.



# KOMPONENTEN AUS UNSEREM PORTFOLIO



## 9. IT-SEC-CHECK

Sie sind unsicher, wie es um die Sicherheit und Qualität Ihrer IT bestellt ist?

Mit unserem netlogix IT-Sec-Check verschaffen Sie sich einen raschen Überblick über Ihre IT-Sicherheit. Unsere erfahrenen IT-Security-Consultants analysieren Ihre IT-Systeme und gleichen die Ergebnisse mit den Vorgaben des BSI (Bundesamt für Sicherheit in der Informationstechnik) ab. Ziehen Sie Vorteile aus der Erfahrung unserer Experten, die bereits in zahlreichen Projekten ihre Kompetenz unter Beweis gestellt haben und machen Sie Ihr Unternehmen cyberresilient!



## 10. RANSOMWARE PROTECTION

Die Ransomware Protection schützt End-points und Server mit ihrer speziellen Crypto-Guard-Technologie, die unbefugte lokale und Remote-Verschlüsselungen von Dateien durch schädliche Software stoppt. Die Daten werden anschließend in Ihren Ursprungszustand zurückversetzt, sodass Erpressungsversuche keine Chance haben.





### 11. SUPA (Security User Program – Awareness)

Wir bieten ein mehrstufiges Awareness-Sicherheitskonzept für Anwender und fördern den bewussten Umgang mit digitalen Bedrohungsszenarien für einen sicheren Arbeitsplatz.

**Impulsvortrag als Kick-Off** – Bewusstsein der Mitarbeiter schärfen mit typischen Szenarien und Tipps fürs Daily Business.

**Know-how mit Online-Trainings aufbauen** – von Security-Trainings, Phishing bis DSGVO individuell abstimmbare.

**Managed Phishing Kampagnen** – täuschend echte Angriffe schulen die Awareness Ihrer Anwender. Jede Kampagne wird in einer detaillierten Übersicht ausgewertet.



### 12. IT-TRAINING

Wir bieten Aus- und Weiterbildungen sowie offizielle Zertifizierungen für IT-Verantwortliche in unserem hauseigenen Trainingscenter an. Schulen Sie Ihre Mitarbeiter von Beginn an richtig und effektiv!



# PERSÖNLICH UND NAH. IHR CLOUD-ANBIETER IN NÜRNBERG.

*Hallo, wir sind nlx.cloud. Ihr leistungsstarker, persönlicher Cloud-Anbieter mit übergreifendem IT-Know-how. Wir konzipieren moderne Architekturen, stellen maßgeschneiderte Cloud-Services bereit und stehen immer persönlich an Ihrer Seite. Mit 20 Jahren Erfahrung betreiben wir sichere, skalierbare Umgebungen für jede Anforderung.*

## **Hohe Verfügbarkeit**

Durch die Spiegelung Ihrer Daten und die Nutzung redundanter Hardware in verschiedenen Brandabschnitten stellen wir eine hohe Verfügbarkeit sicher.

## **Persönliche Betreuung von A bis Z**

Als leistungsfähiger Cloud-Anbieter sind wir von der Umgebungsanalyse über die Konzepterstellung bis zum Betrieb und Support für Sie da.

## **Beliebig skalierbar**

Zahlen Sie nur die Ressourcen, die Sie tatsächlich nutzen, inklusive aller Lizenzen für Hard- und Software. Sie können unsere Services nach Bedarf ganz einfach hinzu buchen oder abwählen.

## **Datenschutz nach deutschem Recht**

IT made in Germany. Wir garantieren Sicherheit nach höchstmöglichen, deutschen Standards.

## **Regionale Rechenzentren**

Think global. Act local. Ihre Daten bleiben vor Ort in regionalen Hochsicherheitsrechenzentren.

## **Hohe Energieeffizienz**

Weil wir möchten, dass Sie große Fußstapfen, aber einen möglichst kleinen ökologischen Fußabdruck hinterlassen, setzen wir auf energieeffiziente Rechenzentren und erneuerbare Energien aus der Region.

# STARK IN DER CLOUD

## UNSERE SERVICES



# SELBSTEINSCHÄTZUNG IHRER CYBERRESILIENZ:

Bewerten Sie jede Frage auf einer Skala von 1 bis 5.

1 = Stimme überhaupt nicht zu und 5 = Stimme vollständig zu.

Addieren Sie am Ende die Punktzahlen, um Ihre Gesamtbewertung zu erhalten.

## 1. SICHERHEITSBEWUSSTSEIN:

Wie oft werden Ihre Mitarbeiter in Bezug auf aktuelle Cyberbedrohungen und Best Practices geschult?

- Selten bis gar nicht [1] | 
  Gelegentlich [2] | 
  Durchschnittlich [3] | 
  Häufig [4] | 
  Regelmäßig und intensiv [5]

## 2. NOTFALLVORBEREITUNG:

Haben Sie einen gut dokumentierten Notfallwiederherstellungsplan für den Fall eines Cyberangriffs?

- Nein, gar nicht [1] | 
  Ja, aber er ist veraltet oder unvollständig [2] | 
  Ja, aber er wurde vor langer Zeit erstellt [3] | 
  Ja, er wurde vor Kurzem überarbeitet [4] | 
  Ja, er ist aktuell und umfassend [5]

## 3. DATENVERSCHLÜSSELUNG:

Werden sensible Daten und Kommunikation innerhalb Ihres Unternehmens verschlüsselt?

- Nie [1] | 
  Selten [2] | 
  Gelegentlich [3] | 
  Häufig [4] | 
  Immer [5]

## 4. NETZWERKSICHERHEIT:

Wie oft werden Sicherheitsüberprüfungen und Penetrationstests für Ihre Netzwerke und Systeme durchgeführt?

- Nie [1] | 
  Selten [2] | 
  Jährlich [3] | 
  Halbjährlich [4] | 
  Vierteljährlich oder öfter [5]

## 5. REGELMÄSSIGE AKTUALISIERUNGEN:

Werden Software, Betriebssysteme und Sicherheitspatches regelmäßig und zeitnah aktualisiert?

- Selten oder nie [1] | 
  Gelegentlich [2] | 
  Meistens [3] | 
  Fast immer [4] | 
  Immer [5]

**6. ZUGRIFFSKONTROLLE:**

Verfügen Sie über strenge Zugriffskontrollen für Ihre IT-Ressourcen und Daten?

- Nein, gar nicht [1] | 
  In begrenztem Umfang [2] | 
  Teilweise [3] | 
  Überwiegend [4] | 
  Vollständig [5]

**7. EXTERNE PARTNERSCHAFTEN:**

Werden auch die Sicherheitspraktiken und -standards Ihrer externen Partner überprüft?

- Nie [1] | 
  Selten [2] | 
  Gelegentlich [3] | 
  Meistens [4] | 
  Immer [5]

**8. INCIDENT RESPONSE:**

Haben Sie klare Verfahren für den Umgang mit Cyberangriffen und Datenschutzverletzungen?

- Nein, nicht vorhanden [1] | 
  Ja, aber sie sind nicht ausreichend [2] | 
  Ja, teilweise [3] | 
  Ja, gut etabliert [4] | 
  Ja, sehr robust [5]

**9. RISIKOBEWERTUNG:**

Wird regelmäßig eine umfassende Bewertung Ihrer IT-Risiken durchgeführt?

- Nie [1] | 
  Selten [2] | 
  Gelegentlich [3] | 
  Jährlich [4] | 
  Mehrmals im Jahr [5]

**10. MITARBEITERENGAGEMENT:**

Sind Ihre Mitarbeiter aktiv in die Cyberresilienz-Strategie Ihres Unternehmens eingebunden?

- Nein, überhaupt nicht [1] | 
  Wenige sind involviert [2] | 
  Einige sind involviert [3] | 
  Die meisten sind involviert [4] | 
  Alle sind aktiv beteiligt [5]

**IHRE PUNKTZAHL****INTERPRETATION DER PUNKTZAHL:**

**10-20 Punkte:** Niedrige Cyberresilienz, Verbesserungsbedarf

**21-30 Punkte:** Mittlere Cyberresilienz, einige gute Praktiken, aber Verbesserungspotenzial

**31-40 Punkte:** Gute Cyberresilienz, solide Praktiken und Vorbereitung

**41-50 Punkte:** Hohe Cyberresilienz, starke Sicherheitsmaßnahmen und Bereitschaft



#### IT-SERVICES

Kompetent, innovativ und einfach in der Zusammenarbeit.

#### IT-TRAINING

Seminare, Workshops und individuelle Schulungen mit vielen Serviceleistungen.

#### WEB SOLUTIONS

Digitalisierung beginnt im Web. Welcome to the Digital Platform Architects.

#### NLX.CLOUD

Persönlich und nah. Ihr Cloud-Anbieter in Nürnberg.

**Haben Sie Fragen?**

*info@netlogix.de*

**Besuchen Sie unsere Website**

*it-services.netlogix.de*

■ IT-SERVICES ■ IT-TRAINING ■ WEB SOLUTIONS ■ NLX.CLOUD

