ANTARES
NETLOGIX

IT-ÜBERPRÜFUNGEN

KENNEN SIE DAS SICHERHEITSLEVEL IHRER IT?

Das erfahrene Antares Red Team überprüft Ihre IT-Systeme und IT-Organisation auf Herz und Nieren, von der technischen und organisatorischen Sicherheit über die Datensicherheit bis hin zur Compliance. **Regelmäßige Risiko- und Schwachstellen-analysen nach nationalen und internationalen Standards** und eine laufende Kontrolle der bereits getroffenen Vorkehrungen schützen Ihr Unternehmen.

ANTARES NETLOGIX
Antares-NetlogiX Netzwerkberatung GmbH
Feldstraße 13, A-3300 Amstetten
T: +43 74 72 / 65 480-0 E: office@netlogix.at

www.netlogix.at

UNSERE IT-ÜBERPRÜFUNGEN

Erhöhen Sie die Sicherheit auf technischer und organisatorischer Ebene.

Wählen Sie aus unseren Modulen und unterziehen Sie Ihre IT dem Härtetest.

Verschaffen Sie sich einen Überblick über das Sicherheitslevel der Systeme, Anwendungen, Infrastruktur und über das Security-Bewusstsein Ihrer Mitarbeiter.

1 EXTERNE SICHERHEITSÜBERPRÜFUNGEN

+ 1.1 Externer Penetrationstest
Sind technische Angriffe auf das Unternehmen von außen möglich?

+ 1.2 Web-Application-Penetrationstest
Wir identifizieren die Schwachstellen in Web-Anwendungen.

+ 1.3 Mobile-App-Penetrationstest
Sicherheitsüberprüfung mit besonderem Augenmerk auf vertrauliche Daten. Nur für Android.

+ 1.4 Denial-of-Service-Penetrationstest
Wir testen, ob Ihre Server anfällig für Denial-of-Service-Angriffe sind.

+ 1.5 Phishing-Kampagnen
Überprüfen Sie das Sicherheitsbewusstsein Ihrer Mitarbeiter mit einer Phishing-Kampagne.

2 INTERNE SICHERHEITSÜBERPRÜFUNGEN

+ 2.1 Interner Penetrationstest
Simulation und Kombination von Angriffstechniken im internen Netz.

+ 2.2 WLAN-Penetrationstest
Wir überprüfen Ihre Funknetzwerke hinsichtlich der eingesetzten Authentifizierungsmethoden und Verschlüsselungsalgorithmen.

+ 2.3 VoIP-Penetrationstest
Wir überprüfen, ob Ihre Kommunikation ausreichend gesichert ist.

+ 2.4 Penetrationstest Produktionsumgebung
Wir überprüfen die Sicherheit Ihrer Produktions-, SCADA- oder OT-Infrastruktur.

+ 2.5 Social Engineering
Wir versuchen vor Ort, sensible Informationen über das Unternehmen zu erhalten.

3 INFRASTRUKTUR-AUDITS

+ 3.1 Verfügbarkeits- und Infrastruktur-Audit
Wir überprüfen Ihre IT-Infrastruktur auf Herz und Nieren. Am Ende steht immer ein abgestimmter Maßnahmenplan, durch dessen Umsetzung die verfolgten Ziele erreicht werden können.

+ 3.2 Firewall Review
Unsere Experten nehmen Ihr Firewall-Regelwerk genauestens unter die Lupe!

+ 3.3 Microsoft 365 Entra ID Review
Review der Konfigurationseinstellungen nach Microsoft best Practices.

+ 3.4 Code Review
Unsere Experten überprüfen die Portal-Integration sowie die Betriebssystem-Security.

4 COMPLIANCE & ORGANISATION

+ 4.1 Organisations-Audit
Wir überprüfen Ihre IT-Sicherheitspolitik inkl. Risikoanalyse.

+ 4.2 Incident Response Audit
Sind Sie ausreichend auf IT-Sicherheitsvorfälle vorbereitet?

+ 4.3 Datenschutz-Audit nach EU-DSGVO
Wir erheben für Sie den IST-Stand und die organisatorischen & technischen Anforderungen.

+ 4.4 Audit nach IEC 62443
Wir erheben für Sie den IST-Stand und die organisatorischen & technischen Anforderungen.

+4.5 Reifegradanalyse NIS2
Wir identifizieren betroffene Systeme & unterstützen bei der Entwicklung eines Maßnahmenplans.

+ 4.6 Audit von IT-Projekten
Erhebung des organisatorischen & technischen Projektstatus nach Projektabschluss, zur Ermittlung des Projektstandes oder für Projekte in der Krise.

MANAGEMENT-PRÄSENTATION

Wir bereiten alle Ergebnisse der Überprüfung in Form einer Präsentation für das Management auf.

1 EXTERNE SICHERHEITSÜBERPRÜFUNGEN

Durch Änderungen an Systemen können neue Sicherheitslücken in der IT-Infrastruktur entstehen. Bei einer externen Sicherheitsüberprüfung werden die technischen Angriffsvektoren auf das Unternehmen von außen überprüft. **Sie erhalten einen Überblick über das Sicherheitslevel der Systeme, Web-Aapplikationen und Ihrer, von außen sichtbaren, IT-Infrastruktur.**

1.1 EXTERNE SICHERHEITSÜBERPRÜFUNGEN

Sind technische Angriffe auf das Unternehmen von außen möglich? Mit einem externen Penetrationstest werden technische Angriffsvektoren auf das Unternehmen von außen überprüft und Sie erhalten einen kompletten Überblick über Ihr Sicherheitslevel.

Ablauf externer Penetrationstest:

- Information Gathering
- Portscan & Dienstidentifikation
- Teilautomatisierte Identifikation von Schwachstellen
- Manuelle Identifikation von Schwachstellen
- Angriffsversuche auf Management-Interfaces
- Verifikation & Ausnutzung der Schwachstellen

1.2 WEB-APPLICATION-PENETRATIONSTEST

Wir identifizieren Schwachstellen in Web-Anwendungen. Wenn Sie eine Webseite oder einen Online-Shop verwalten, sind Sie ein potenzielles Ziel für Angriffe. Die Grundlage für den sicheren Betrieb von Web-Applikationen ist die konsequente Validierung sämtlicher übermittelter Daten. An diesem Punkt setzt das Antares Red Team an. Können Sie Angriffe abwehren?

Ablauf Web-Application-Penetrationstest:

- Information Gathering
- Session Security
- Testen auf sichere Parametervalidierung (Injection, Inclusion, Fuzzing, Cookies)
- Testen der Authentifizierungsmethoden
- Unautorisierte Upload-Versuche
- Kombinierte Angriffsszenarien
- Teilautomatisierte Identifikation bekannter Schwachstellen in der Server-Software
- Prüfung der Webserver-Konfiguration

1.3 MOBILE-APP-PENETRATIONSTEST

Sind Sie sicher, dass Ihre mobilen Apps sicher sind? Mobile Applikationen stellen besondere Sicherheitsherausforderungen dar. Wir überprüfen die Sicherheit mobiler Apps mit besonderem Augenmerk auf die Übertragung vertraulicher Daten. Nur für Android.

Folgende Fragen klärt der Mobile-App-Penetrationstest:

- Ist es möglich, unerlaubte Daten einzuschleusen?
- Reagiert die Software adäquat auf illegale Dateneingaben?
- Sind Netzwerkverbindungen kryptografisch sicher?
- Sind Datenformate korrekt und sicher?
- Sind Rechte/Berechtigungen korrekt gesetzt?
- Welche Dateien befinden sich in dem Paket?

1.4 DENIAL-OF-SERVICE-PENETRATIONSTEST

Sind Ihre Server anfällig für Denial-of-Service-Angriffe? DOS-Attacken werden mittlerweile von Cyber-Kriminellen zum Kauf angeboten, um Konkurrenten zu schädigen. Wir überprüfen, ob die implementierten Schutzmaßnahmen korrekt funktionieren.

Ablauf Denial-of-Service-Penetrationstest:

- Volumenbasierte Angriffe
- Protokollangriffe
- Applikationsangriffe

1.5 PHISHING-KAMPAGNEN

Cyberkriminalität, Spionage und Hacker stellen ernsthafte Bedrohungen dar. Ihre Systeme sind vielleicht gut gesichert, aber was ist mit Ihren Mitarbeitern? Eine häufige Methode von Hackern, um sich den Weg in das Unternehmensnetzwerk zu bahnen, sind Phishing-Attacken. **Überprüfen Sie das Sicherheitsbewusstsein Ihrer Mitarbeiter.**

Ablauf Phishing-Kampagne:

- Generische Phishing-E-Mails: gefälschte E-Mail-Nachrichten (angepasst an größere Plattformen wie Office 365 oder Xing)
- Gezielte Phishing-E-Mails: gefälschte E-Mail-Nachrichten anhand eines internen Templates

2 INTERNE SICHERHEITSÜBERPRÜFUNGEN

Durch interne Sicherheitsüberprüfungen werden alle möglichen Angriffsvektoren auf das Unternehmen von innen überprüft. **Sie erhalten einen Überblick über das Sicherheitslevel Ihrer internen IT-Systeme und über das Security-Bewusstsein Ihrer Mitarbeiter.**

2.1 INTERNER PENETRATIONSTEST

Aufgrund steigender Bedrohung für Unternehmen durch Angreifer aus dem internen Netzwerk, aber auch durch Schadsoftware, **ist es essenziell, die internen Systeme regelmäßig einer Prüfung zu unterziehen**. Nur dadurch kann die Verfügbarkeit Ihrer Systeme sichergestellt werden. Wir simulieren und kombinieren Angriffstechniken im internen Netz. Welche Möglichkeiten haben Angreifer oder Malware, wenn es gelingt, ins interne Netz vorzudringen?

Mögliche Ablaufvarianten:

- BLACKBOX: Wir wissen nicht, welche Systeme zu erwarten sind, und haben keine Informationen über die IT-Infrastruktur.
- GRAYBOX: Es werden die zu testenden IP-Bereiche festgelegt und möglicherweise bestimmte Systeme ausgeschlossen.
- WHITEBOX: Hier sind wir im Vorfeld der Überprüfung über die IT-Infrastruktur informiert. Da der Tester alle Informationen hat, ist die Effektivität viel höher als bei einem BLACKBOX-Penetrationstest.

2.2 WLAN-PENETRATIONSTEST

Sind Sie sicher, dass unbefugte Personen keinen Zugriff zum Netzwerk erhalten? Wir überprüfen die verfügbaren Funknetzwerke hinsichtlich der eingesetzten Authentifizierungsmethoden und Verschlüsselungsalgorithmen.

Ablauf WLAN-Penetrationstest:

- Überprüfung der implementierten Verschlüsselung
- Prüfung von Abschottung und Filterung des WLANs
- Wardriving/Warwalking
- Identifikation unternehmensfremder Funknetzwerke

2.3 VOIP-PENETRATIONSTEST

Wir überprüfen, ob Ihre Kommunikation ausreichend gesichert ist. Der Einsatz und die Verfügbarkeit von VoIP im Unternehmensumfeld ist von großer Bedeutung. Es ergeben sich jedoch Bedrohungsszenarien auf verschiedenen Ebenen. Mit uns können Sie sicher sein, dass ein Konferenztelefon kein Eigenleben entwickelt, wenn der Vorstand tagt.

2.4 PENETRATIONSTEST VON PRODUKTIONSUMGEBUNGEN

Wir überprüfen die Sicherheit Ihrer Produktions-, SCADA- oder OT-Infrastruktur. Von der Überprüfung des Zugangsschutzes und der Konfigurationsschwachstellen der Anbindung des Netzwerkes über Angriffe auf Server-, Netzwerk- und Feldkomponenten bis hin zum Versuch, den physikalischen Zugriff zu erlangen. Dabei gehen wir sehr sorgfältig vor, um die Verfügbarkeit nicht zu beeinträchtigen.

2.5 SOCIAL ENGINEERING

Ihre Systeme sind vielleicht gut gesichert, aber was ist mit Ihren Mitarbeitern? Ein unaufmerksamer Mitarbeiter kann - ohne es zu wissen - sehr leicht die digitale Tür für Hacker öffnen. Mit unserem Awareness-Test erfahren Sie, ob und wie weit Ihre technische Infrastruktur einem Angriff standhält, ob die Alarmfunktionen, Prozesse und Abläufe genügen und ob Ihre Mitarbeiter ausreichend sensibilisiert sind. Gerade im Bereich des Social Engineerings sind die Möglichkeiten, über die Schwachstelle Mitarbeiter Zugriff zu internen Systemen oder sensiblen Informationen zu erlangen, sehr vielfältig.

Mögliche Angriffsszenarien:

- Vortäuschen falscher Identitäten und Kompetenzen, um an geheime Daten zu gelangen oder Services zu erschleichen.
- Persönlicher Zugang zu internen Systemen, indem wir uns als Servicetechniker oder ähnliches ausgeben.

3 INFRASTRUKTUR-AUDITS

„Das Netz ist so langsam." Es ist überraschend, wie leidensfähig viele User und Firmenkunden sein können. Unsere Spezialisten beheben in wenigen Stunden die Probleme, die Sie bereits seit Monaten beschäftigen. Fehlkonfigurationen bei Netzwerkkomponenten und fehlende Argumente sind zumeist die Ursache bei Diskussionen mit Software-Herstellern oder Providern über instabile Systeme. **Wir finden die Fehler, unterstützen Sie bei der Problembehebung und sorgen wieder für einen reibungslosen Betrieb.**

3.1 VERFÜGBARKEITS- UND INFRASTRUKTUR-AUDIT

Die Ursachen für Leistungsdefizite können vielfältig sein und reichen buchstäblich von verstaubten Steckverbindungen bis zu nicht ausreichend dimensionierten Netzwerken. **Wir überprüfen Ihre IT-Infrastruktur auf Herz und Nieren!** Am Ende steht ein abgestimmter Maßnahmenplan, durch dessen Umsetzung die verfolgten Ziele erreicht werden können.

Mögliche Ablaufvarianten:

- Physische RZ-Infrastruktur/Topologie
- Bauliche Gegebenheiten, Brandschutz, Zugangsschutz
- Netzwerktopologie (WLAN, LAN)
- Storage-Infrastruktur
- Visualisierung/Server-Infrastruktur
- Backup-/Restore-Konzeption
- Applikationslandschaft
- Client-Infrastruktur
- Betriebsprozesse
- Service Levels, Wartungsverträge, Support-Verträge
- Gesamtbewertung, Redundanz und Verfügbarkeit

3.2 FIREWALL-REVIEW

Unsere Experten nehmen Ihr Firewall-Regelwerk genauestens unter die Lupe! Unsere zertifizierten Experten überprüfen, ob Regeln entsprechend gewartet sind und die Vergabe der minimal notwendigen Rechte umgesetzt wurde. Im Anschluss erhalten Sie von uns eine Dokumentation und Empfehlung für Gegenmaßnahmen.

Ablauf eines Firewall-Reviews:

- Basis-Review
- Review Benutzer- und Adminrechte
- Review Security-Profile
- Weitere Analysen

3.3 MICROSOFT 365 ENTRA ID REVIEW

Microsoft 365 ist in vielen Unternehmen zum Herzstück der Infrastruktur geworden. Wir überprüfen Ihre Sicherheitseinstellungen und gleichen Handlungsempfehlungen ab. Alle diese Punkte werden in einem Dokument zusammengetragen und Ihnen nach Abschluss zur Verfügung gestellt.

3.4 CODE-REVIEW

Wir überprüfen die Sicherheit Ihrer Applikationen und führen einen unabhängigen Code-Review Ihrer Software oder einzelner Software-Module durch. Der Fokus liegt auf der Sicherheit innerhalb der Applikation, sowie der Netzwerkkommunikation mit anderen Applikationen bzw. Prozessen. Wir dokumentieren Schwachstellen und zeigen Code-Teile mit Verbesserungspotenzial auf, um Ihre Anwendungen robuster zu machen.

IHRE NOTIZEN

4 ORGANISATION & COMPLIANCE

Organisation, Sicherheit und Compliance: Diese Themen unter einen Hut zu bringen, ist die höchste Kunst. **„Technisch-organisatorische Maßnahmen“** sind nicht nur beim Datenschutz das geflügelte Wort, sondern auch im alltäglichen IT-Betrieb eines Security-Operations-Centers oder in einer größeren Support-Organisation.

4.1 ORGANISATIONS-AUDIT

Um Schwachstellen zu erkennen, bedarf es einer Betrachtung „von außen“, die objektiv die Systemkonfiguration und Schutzmaßnahmen überprüft. **Wir überprüfen Ihre IT-Sicherheitspolitik und Statusdokumentation und führen eine Risikoanalyse durch.** Sind die Verantwortlichkeiten geregelt? Gibt es ein Sicherheits-Management-Team?

Die Überprüfung sowie Statusdokumentation erfolgt unter folgenden Aspekten:

- Verantwortlichkeiten & IT-Organisation
- Sicherheits-Management-Team
- Risikoanalyse
- Datenklassifizierung & Datenintegrität
- Reporting

4.2 INCIDENT RESPONSE AUDIT

Sind Sie ausreichend auf IT-Sicherheitsvorfälle vorbereitet? Wir erheben mit Ihnen den IST-Stand der aktuellen Sicherheitsvorkehrungen. Gemeinsam werden Ziele definiert, neue Sicherheitsmaßnahmen nach Best Practices entwickelt und langfristige Strategien geplant. Wir betreuen Sie im gesamten Projekt und Sie erhalten wertvolle Empfehlungen und Tipps zu technischen und strategischen Maßnahmen.

4.3 DATENSCHUTZ-AUDIT NACH EU-DSGVO

Wir erheben den IST-Stand, die organisatorischen Anforderungen und liefern Vorschläge für konkrete Maßnahmen, um eine zukunftssichere, rechtliche und technische Absicherung zu gewährleisten (auf Basis der EU-DSGVO). Mit dieser Struktur können Sie die nächsten Schritte mit internen Ressourcen oder auch mit bestehenden Partnern umsetzen. **Ziel des Audits ist die Konvergenz von Recht, IT und Organisation.**

- Erhebung des IST-Standes bezüglich geltendem Datenschutzgesetz.
- Erhebung der organisatorischen Anforderungen mit Vorstand und Firmenjuristen.
- Einführung organisatorischer Maßnahmen in Abstimmung mit dem Betriebsrat.
- Vorschläge für zukunftssichere rechtliche und technische Absicherung.
- Vorschläge konkreter Maßnahmen und Durchführung von Schulungen für Mitarbeiter.
- Nach Empfehlung auch Einführung von Software-Lösungen.

4.4 AUDIT NACH IEC 62443-STANDARD

Begriffe wie Industrie 4.0 oder IoT stehen für den Beginn eines neuen Zeitalters und die Vision einer durchgängigen Digitalisierung aller Produktionsprozesse. **Wir erheben den IST-Stand & die organisatorischen/technischen Anforderungen nach IEC 62443.**

4.5 REIFEGRADANALYSE NIS2

Wir identifizieren betroffene Systeme & unterstützen bei der Entwicklung eines Maßnahmenplans.

- Identifikation der betroffenen Systeme
- Gap-Analyse zur Identifizierung von Lücken zu den NIS2-Anforderungen
- Entwicklung eines Maßnahmenplans zur Schließung identifizierter Gaps
- Unterstützung bei der Implementierung durch unsere Experten

4.6 AUDIT VON IT-PROJEKTEN

Nach einem Projektabschluss, zur Ermittlung des Projektstandes oder für Projekte in der Krise kann es notwendig sein, den **organisatorischen und technischen Projektstatus zu erheben und zu bewerten.** Wir unterstützen Sie und liefern Ihnen eine Bewertung und Empfehlung.

- Erhebung Projektstatus organisatorisch
- Erhebung Projektstatus technisch
- Bewertung (Soll-/Ist-Gegenüberstellung)
- Empfehlungen (organisatorisch und technisch)

UNSERE EXPERTEN

Setzen Sie auf unser Know-How.

Alle unsere Überprüfungen werden von unseren Experten mit langjähriger Erfahrung und Expertise durchgeführt. Die umfassende Dokumentation und das Reporting sind ein großer Bestandteil der jeweiligen Überprüfung.

Der Auftraggeber hat nach jeder Überprüfung eine umfassende Entscheidungsgrundlage zur Verfügung und kann somit konkret planen, wo Verbesserungen der Systeme vorgenommen werden sollten.

ANTARES RED TEAM

Unter der Leitung von Security-Spezialist und CISSP Stefan Winkler führt das **ANTARES RED TEAM** zahlreiche Audits und Penetrationstests durch.

Alle Mitglieder des Antares Red Teams verfügen über einschlägige Erfahrung und fundierte Kenntnisse in verschiedensten Bereichen der IT-Sicherheit und Infrastruktur.

In den Teams ergänzen sich unsere Experten mit ihren individuellen Kompetenzen und Expertisen optimal und konnten bisher jedes IT-System bezwingen.

WAS IST EIN RED TEAM?

Red Team ist ein Begriff aus dem Bereich der IT-Sicherheit. Red Teams führen Sicherheits- und Penetrationstests aus der Perspektive echter Angreifer durch. Sie versuchen an sensible Daten zu gelangen oder in IT-Systeme und -Netzwerke einzudringen.

COMPLIANCE

DI (FH) Gerhard Kratschmar ist es als ehemaliger Berufspilot gewohnt, strukturiert vorzugehen, Prozesse zu erstellen und diese strikt einzuhalten.

Als **zertifizierter Datenschutzbeauftragter**, **CISSP** und **Auditor nach ISO 27001** bei Antares-NetlogiX sowie **Safety & Security Manager** im weltweiten Einsatz, unterstützt Sie Gerhard Kratschmar im Bereich Organisation und Compliance.

Gehard Kratschmar steht auch als **Chief Information Security Officer** zur Verfügung.

Was bietet Ihnen CISO-as-a-Service:

Mit unserem Service können Sie die Strategie Ihrer Sicherheitsmaßnahmen auslagern, damit Ihre Informationssicherheitsprojekte angemessen begleitet werden.

Rent-a-CISO ist unsere Antwort auf hohe Gehaltskosten.

UNSERE ERFAHRUNGEN

Wir haben uns als führendes IT-Beratungsunternehmen und Managed Security Service Provider etabliert und betreuen zahlreiche Top-Unternehmen. Netzwerke und Security sind seit der Gründung von Antares-NetlogiX im Jahr 2000 unsere Kernkompetenzen.

HUECK FOLIEN

„Wir waren auf der Suche nach einem verlässlichen kompetenten Partner, welcher uns in Sachen IT-Security unterstützen sollte. Die Wahl fiel dabei auf Antares NetlogiX. Im Nachhinein betrachtet war es eine sehr gute Entscheidung!“

Wolfgang Naderer, Informationstechnologie | HUECK FOLIEN

WIR SIND IHR PARTNER

Vertrauen Sie auf unsere Expertise.

Wir empfehlen regelmäßige Überprüfungen!

UNSERE ERFAHRUNG

Seit mehr als 15 Jahren führen wir Penetrationstests sowie Sicherheits- und Organisations-Audits durch.

STANDARDS

Halten Sie mit uns Compliance-Vorgaben & internationale Standards ein (z. B. PCI DSS, IEC 62443, ISO 27001, EU-DSGVO, NIS-Richtlinie).

DOKUMENTATION

Alle Schritte und gefundenen Schwachstellen werden gewissenhaft dokumentiert und in einem ausführlichen Report zusammengefasst.

ERGEBNISSE

Nach Abschluss der Überprüfung erhalten Sie von uns konkrete Ergebnisse, Empfehlungen und Verbesserungsvorschläge, um etwaige Sicherheitsrisiken zu beheben.

MASSNAHMEN

Unsere Experten verfügen über umfassendes Know-how. Wir beraten und betreuen Sie auch bei der Umsetzung der empfohlenen Maßnahmen im Anschluss.

ERHÖHEN SIE IHRE SICHERHEIT

Das Ziel einer Sicherheitsüberprüfung ist es, Sicherheitslücken aufzudecken, zu dokumentieren und somit Lösungsmöglichkeiten aufzuzeigen, um für eine erstklassige IT-Sicherheit zu sorgen.

360° SECURITY SERVICES

Alle unsere Sicherheitsüberprüfungen werden auch als **Managed Security Services** angeboten.

Vermindern Sie das Risiko, schonen Sie Ressourcen und nutzen Sie beispielsweise den Vorteil einer **regelmäßigen Schwachstellenanalyse**. Unser Team steht Ihnen für Fragen jederzeit gerne zur Verfügung.

DER HÄRTETEST FÜR IHRE IT-SICHERHEIT

Wie gut ist Ihr Unternehmen gegen Hacker-Angriffe aller Art geschützt? Mit unseren Sicherheitsüberprüfungen und Penetrationstests erhalten Sie die Antwort. Nach jeder Überprüfung steht Ihnen eine umfassende Entscheidungsgrundlage zur Verfügung und Sie können somit konkret planen, wo Verbesserungen der Systeme vorgenommen werden sollten.

1. Klärung der **Erwartungshaltung** und Zieldefinition
2. Ausführliche **Recherche** über die Zielsysteme
3. Aktive **Überprüfung der Systeme** durch unsere Experten
4. Konkrete **Abschluss-bewertung** und **Ergebnispräsentation**
5. Zusätzlich abschließende **Folgeüberprüfung**

Weitere Informationen finden Sie auf unserer Website

ANTARES RED TEAM

www.netlogix.at

ANTARES NETLOGIX

Antares-NetlogiX Netzwerkberatung GmbH
Feldstraße 13, A-3300 Amstetten
T: +43 74 72 / 65 480-0 E: office@netlogix.at

06 02 2024