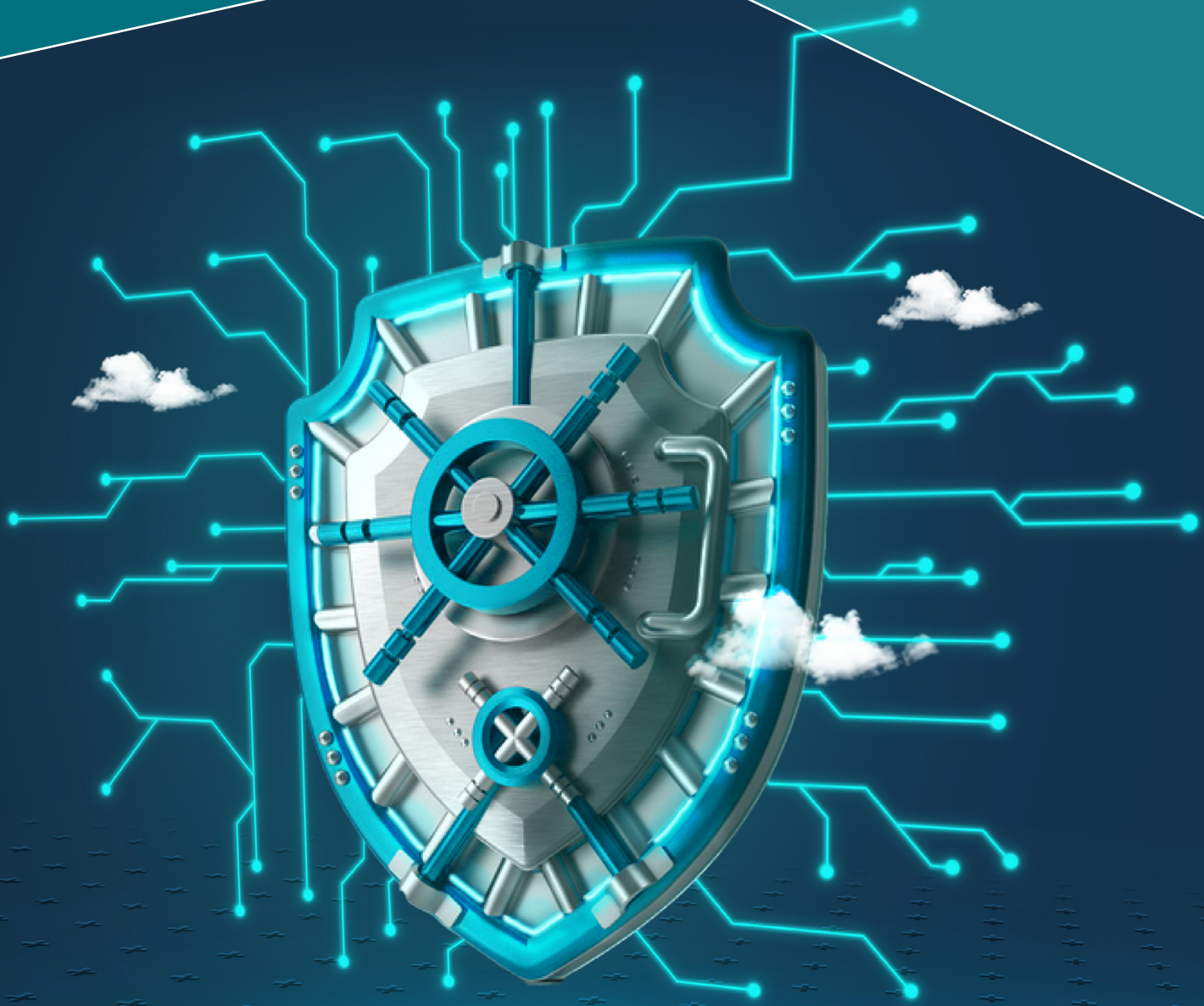
IHRE IT IN SICHEREN HÄNDEN:

Cybersicherheit auf höchstem Niveau!



INCAS

MEMBER OF THINK ABOUT IT

IST IHRE ORGANISATION AUSREICHEND GESCHÜTZT?

Cyberbedrohungen in einer vernetzten Welt: Aktuelle Erkenntnisse und Empfehlungen

Digitale Technologien spielen in unserer Gesellschaft eine zunehmende zentrale Rolle. Organisationen sind mehr denn je den Risiken von Cyberbedrohungen ausgesetzt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) liefert in seinem Lagebericht wichtige Erkenntnisse und Empfehlungen, um den Bedrohungen proaktiv zu begegnen und die Sicherheit von IT-Systemen zu gewährleisten. Darunter zählt zum Beispiel:

- Die Identifikation einer Vielzahl von Bedrohungen für Unternehmen und anderen Einrichtungen
- Die Bedeutung von Prävention und proaktiven Sicherheitsmaßnahmen
- Die Bedeutung eines ganzheitlichen Sicherheitsansatzes, der technologische, organisatorische und menschliche Aspekte umfasst

Bundesamt
für Sicherheit in der
Informationstechnik

NIS-2-Richtlinie – Sind Ihre Sicherheitsstandards noch aktuell?

Mit der Einführung der NIS-2-Richtlinie im Oktober 2024 werden für Unternehmen und Organisationen verbindliche Sicherheitsstandards und Meldepflichten eingeführt. Ziel ist, ein höheres gemeinsames Niveau der Cybersicherheit in der EU zu erreichen.

Mit unseren vollumfassenden IT-Security-Services unterstützen wir Sie bei Ihrem Vorhaben und bieten eine Rundum-Lösung, um Ihre IT-Umgebung nach Ihren individuellen Anforderungen und aktueller Gesetzesgrundlage so sicher wie möglich zu gestalten.

Ransomware ist weiterhin die größte Bedrohung für Organisationen:

2 pro Monat

Ransomware-Angriffe auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.

68

erfolgreiche **Ransomware-Angriffe** auf Unternehmen wurden bekannt.

Mehr als

2.000

Schwachstellen in Software-Produkten (15 % davon kritisch) wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein Zuwachs von 24 %.

Eine Viertelmillion

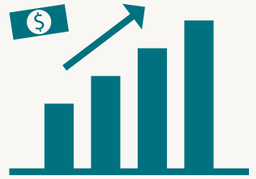
neue Schadprogramm-Varianten wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.

Bedrohungen je Zielgruppe:

Gesellschaft

Identitätsdiebstahl
Erpressung & Phishing

Wirtschaft



Ransomware
Abhängigkeit innerhalb der IT-Supply-Chain

Staat und Verwaltung

Ransomware
Advanced Persistent Threat

84% aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken.

66% aller Spam-Mails im Berichtszeitraum waren Cyberangriffe:
- 34 % Erpressungsmails
- 32 % Betrugmails

Quelle: bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

UNSER LAYER-MODELL

Jetzt kostenlose Beratung anfragen!

Unser Layer-Modell der IT-Sicherheit bietet eine umfassende Struktur zur Planung, Implementierung und Überwachung von Sicherheitsmaßnahmen in Organisationen. Durch die Unterteilung in sieben klar definierte Schichten ermöglicht das Modell eine ganzheitliche Betrachtung der Sicherheitsanforderungen.

Ein holistisches IT-Security Konzept kann vereinfacht wie ein Gebäude mit Zaun, Tür und Schloss bildlich umschrieben werden. Schützen Sie Ihre Einrichtung durch die sieben nachstehenden Ebenen:

1. Human Layer
Schutz durch geschultes Personal

2. Perimeter Security
Absicherung gegen äußere Einflüsse mittels Next Gen Firewall-Systemen

3. Network Security
Sichere Gestaltung Ihres Netzwerks und/oder Multi-Layer Firewalls

4. Endpoint Security
Verschlossene Türen für mehr Sicherheitsverwaltung der Client-Systeme

5. Application Security
Schutz des Herzstückes digitaler Systeme durch Schwachstellenmanagement

6. Data Security
Schutz vor Datenverlust mittels Backups

7. Mission Critical Assets
Ihre zu schützende Ressource für einen reibungslosen Betrieb

Wir bieten Ihnen zu jeder Ebene den passenden Service und beraten Sie umfassend nach Ihren individuellen Anforderungen!

Unser Service für jede Ebene:

1. Managed Cybersecurity Training
Durch die Schulung Ihrer Mitarbeitenden verwandeln wir potenzielle Schwachstellen zu einer starken Barriere gegen eine Vielzahl von Angriffen.

2. Managed Firewall
Unser Managed Firewall Service ermöglicht es Ihnen, Ihre Firewall-Systeme durch professionelle Expertise verwalten zu lassen.

3. Managed Network Access Control (NAC)
NAC-as-a-Service ermöglicht Ihnen, Transparenz und Sichtbarkeit im Netzwerk zu gewinnen und Ihre Sicherheitsmaßnahmen kontinuierlich anzupassen.

4. Managed Detection & Response (MDR)
Unser Managed Detection & Response Service bietet eine umfassende Lösung für die Sicherheitsverwaltung Ihrer Client-Systeme.

5. Vulnerability Management
Unser Service für Schwachstellenmanagement ist ein zentraler Baustein unserer Sicherheitslösungen, der es ermöglicht, potenzielle Sicherheitslücken gezielt zu erkennen und umfassend zu untersuchen.

6. Managed Backup
Unsere Elasticloud Backup Lösung ist eine leistungsstarke Suite von Datenmanagement- und Datensicherungslösungen.

7. Managed Critical Assets
Mit unseren Services rund um IT-Security sichern wir Ihre Organisation vollumfänglich nach Ihren individuellen Anforderungen ab.

Sicherheits-Check: Jetzt anfragen!

E: security@incas.de
T: +49 2151 620 - 1260

Jetzt anfragen

UNSERE SERVICES IM DETAIL

1. Managed Cybersecurity Training

Mehr erfahren

- ✓ **Nachhaltige Lerneffekte:** Interaktive, Story basierte und laufend aktualisierte Module mit differenzierten Lernpfaden
- ✓ **Nachhaltig minimierte Anfälligkeit für Phishing:** Regelmäßige, branchenspezifisch zugeschnittene Phishing-Simulationen
- ✓ **Verhaltensänderung und „Security Culture“:** Basierend auf modernsten psychologischen Mechanismen wie Micro-Learning, Storytelling und Gamification
- ✓ **Erfüllte Compliance-Anforderungen:** Auditfähiges Dashboard und Reporting. Dadurch sind Sie jederzeit bereit für Audits wie ISO 27001 oder BSI-Grundschutz
- ✓ **Skalierbare Individualisierung:** Automatisierte Anpassung der Lerninhalte an Ihre Anforderungen
- ✓ **100 % DSGVO-konform:** Daten werden ausschließlich in der EU verarbeitet

2. Managed Firewall

Mehr erfahren

- ✓ **Verbesserte Sicherheit:** Kontinuierliche Überwachung und Updates
- ✓ **Service Desk:** Minimierung von Ausfallzeiten und schnelle Reaktionen
- ✓ **Kosteneinsparungen:** Weniger Ausgaben für Betrieb und Wartung
- ✓ **Skalierbarkeit:** Leicht anpassbar an wachsende Unternehmensbedürfnisse
- ✓ **Einhaltung von Compliance:** Unterstützung bei der Erfüllung regulatorischer Anforderungen
- ✓ **Detaillierte Berichterstattung:** Klare Analysen und Insights zum Netzwerkverkehr

3. Managed Network Access Control

Mehr erfahren

- ✓ **Zugangsschutz:** Umfassende Kontrolle und Steuerung aller Netzwerkzugänge
- ✓ **Endpoint:** Unterstützung bei der Umsetzung von Compliance-Richtlinien
- ✓ **VLAN-Manager:** Einfache Segmentierung und Verwaltung der Virtual Local Area Networks
- ✓ **Sensor Management System:** Mögliche Einbindung verschiedener Standorte und Verwaltung dezentraler Netzwerkumgebungen
- ✓ **Captive Portal:** Regelung des Netzwerkzugangs von Gast- und Fremdkomponenten
- ✓ **Fingerprinting:** Kombination aus verschiedenen Authentifizierungsmethoden

INCAS ISO 27001 zertifiziert

4. Managed Detection & Response (MDR)

Mehr erfahren

- ✓ **Proaktive Bedrohungserkennung:** Cyberbedrohungen & verdächtiges Verhalten in Echtzeit erkennen
- ✓ **Kontinuierliches Monitoring:** Ständige Überwachung des Netzwerks und der Systeme
- ✓ **Sofortige Reaktionsfähigkeit:** Schnelle Reaktion auf Sicherheitsvorfälle 24/7 durch ein weltweites SOC (Security Operations Center) Team
- ✓ **Anpassungsfähige Prozesse:** Maßgeschneiderte Sicherheitsmaßnahmen & Abläufe für spezifische Unternehmensrisiken
- ✓ **Experten-Teams:** Zugriff auf erfahrene Sicherheitsspezialist*innen und Analyst*innen
- ✓ **Minimierung von Risiken:** Verringert das Risiko von Datenverlust und Reputationsschäden
- ✓ **Modernste Technologien:** Einsatz fortschrittlichster KI basierter Endpoint-Security Lösung

5. Vulnerability Management

Mehr erfahren

- ✓ **Bereitstellung virtueller Appliances:** Zugriff auf virtuelle Appliances in allen Netzsegmenten
- ✓ **Bewertung von Schwachstellen:** Bewertung der Schwachstellen nach ihrer Kritikalität
- ✓ **Erfassung IP-basierender Geräte:** Vollständige Erfassung aller IP-basierten Geräte im Netzwerk
- ✓ **Lösungsvorschläge durch Experten:** Vorschläge zur Behandlung identifizierter Schwachstellen
- ✓ **Regelmäßiger Scan:** Regelmäßige Durchführung von Scans aller Geräte
- ✓ **Behebung von Schwachstellen:** Schwachstellenbehebung im Rahmen eines Wartungsvertrages
- ✓ **Schwachstellentests:** Durchführung von über 150.000 standardisierten Schwachstellentests

6. Managed Backup

Mehr erfahren

- ✓ **Schnelle Wiederherstellung:** Funktionen wie Instant VM Recovery können virtuelle Maschinen innerhalb von Minuten wiederherstellen
- ✓ **Datensicherheit und Verschlüsselung:** Vielfältige Sicherheitsfunktionen, einschließlich der Möglichkeit, Backups zu verschlüsseln
- ✓ **Skalierbarkeit:** Managed Backup kann flexibel an die wachsenden Anforderungen angepasst werden
- ✓ **Cloud-Integration:** Möglichkeit Daten in der Cloud zu sichern und wiederherzustellen

E: security@incas.de
T: +49 2151 620 - 1260

Jetzt anfragen

INCAS
MEMBER OF THINK ABOUT IT

Lassen Sie sich von uns beraten!

Jetzt anfragen

Für Fragen stehen wir Ihnen gerne zur Verfügung:

E: security@incas.de | T: +49 2151 620 - 1260