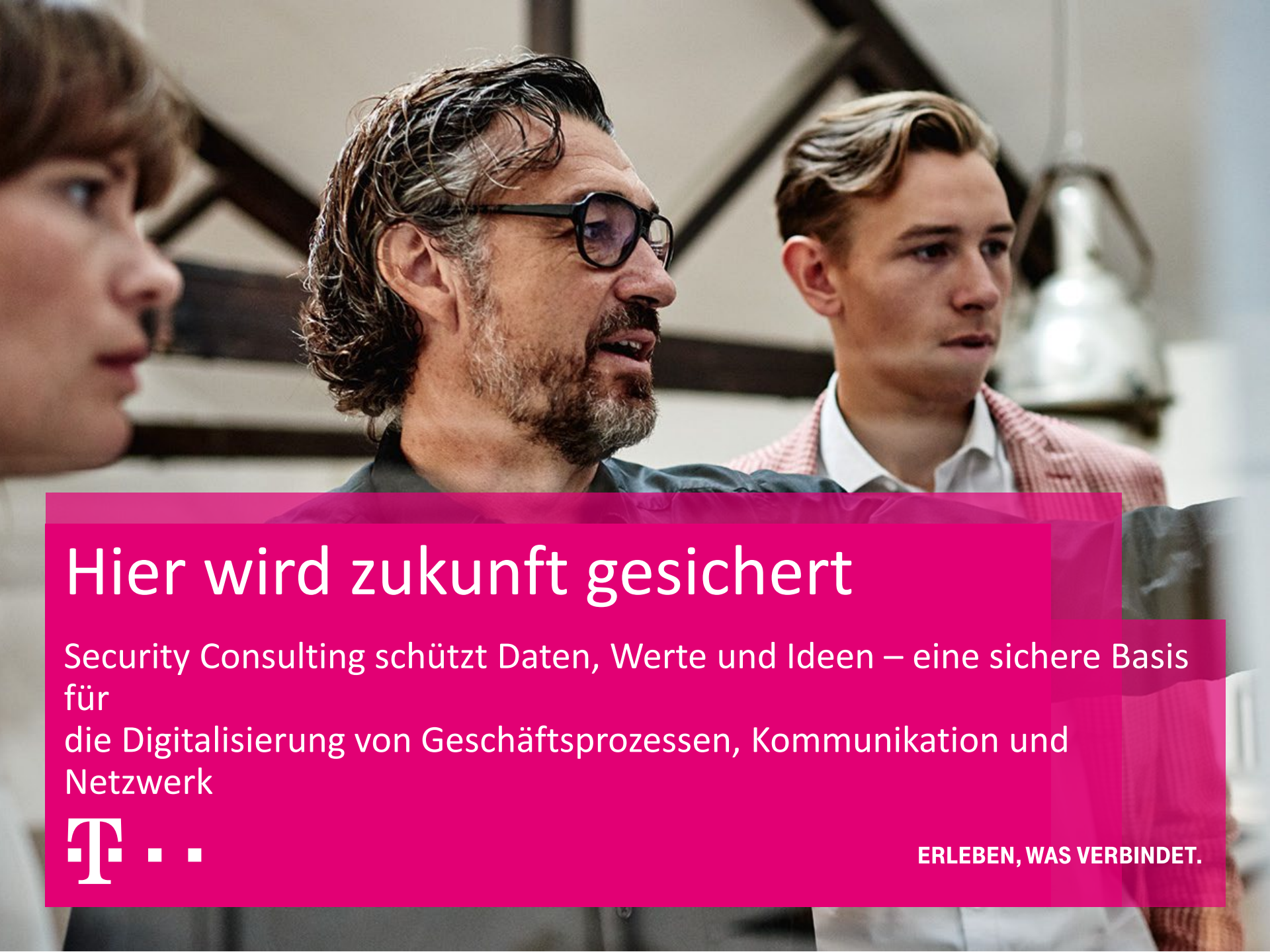
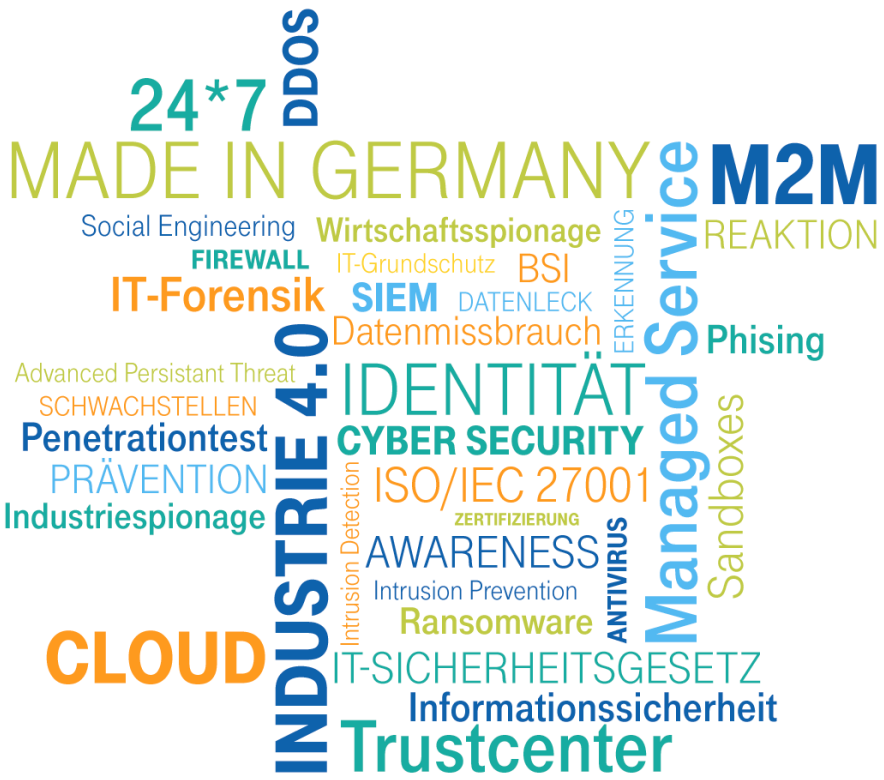


Hier wird zukunft gesichert

Security Consulting schützt Daten, Werte und Ideen – eine sichere Basis für
die Digitalisierung von Geschäftsprozessen, Kommunikation und Netzwerk

ERLEBEN, WAS VERBINDET.

IT-security ist kein zustand
DIe Risiken sind dynamisch – die Lösungen auch



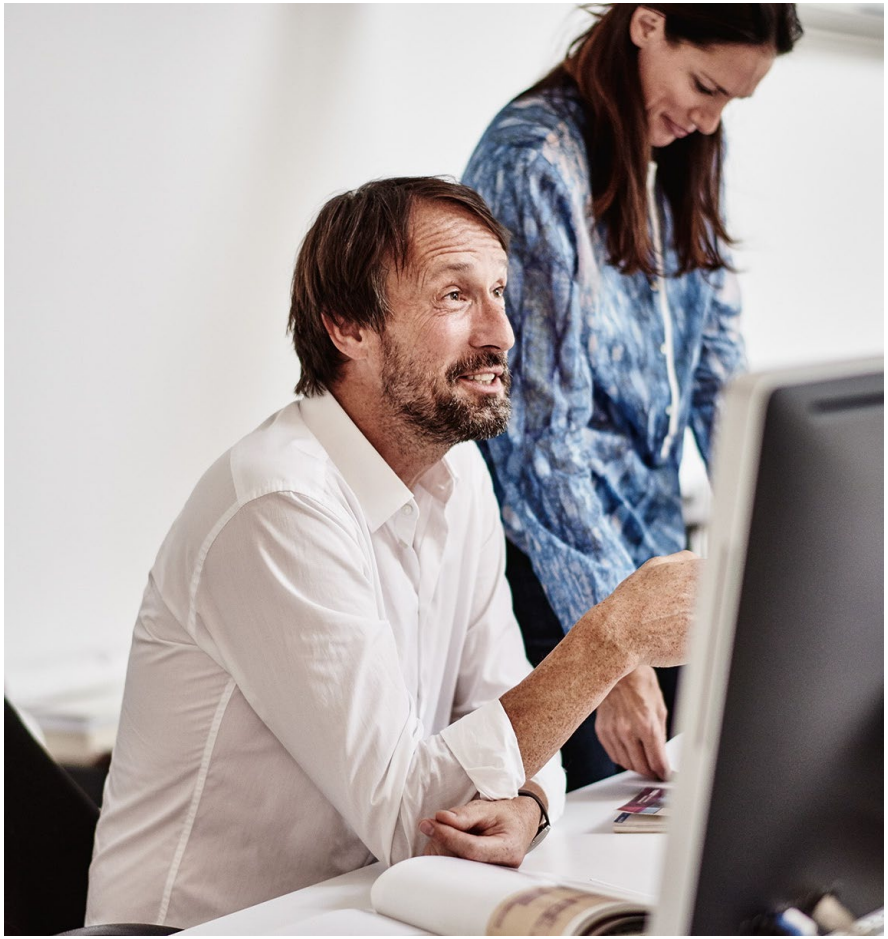
Das macht effektive IT-Sicherheit aus:

- Sie hält Schritt mit der Komplexität der IT-Landschaft
- Sie bietet Antworten auf neue Security-Anforderungen,
  die durch die Digitalisierung entstehen
- Sie kann auf die täglich neuen Security-Gefahrenmeldungen schnell und effektiv reagieren
- Sie hilft, Implementierungs- und Integrationsaufwand sowie Update-Kosten im Griff zu behalten
- Sie begrenzt auch die Betriebs- und Lizenzkosten der IT
- Sie wird permanent sowie situationsgerecht konzipiert und betrieben – durch kontinuierlich geschulte Experten aus dem Unternehmen oder von spezialisierten Dienstleistern
- Sie sensibilisiert auch alle übrigen Mitarbeiter für einen sicheren Umgang mit Endgeräten und Anwendungen

IT-security ist mehr als technologie
wir begleiten sie sicher in die digitale zukunft

Gemeinsam stärker – mit Security Consulting:

- Nutzen Sie unsere objektive Außensicht auf Ihre bisherigen Schutzmaßnahmen und eventuell bestehende Risiken
- Machen Sie sich frei von der Sorge, wie notwendige Erneuerungen bewerkstelligt werden können
- Holen Sie sich unser langjähriges Know-how und unser immer aktuelles Wissen in Sachen IT-Security ins Haus
- Erreichen Sie mit uns ein ganz anderes Sicherheitsniveau
  als allein – lassen Sie uns die Kräfte effektiv bündeln
- Profitieren Sie von konstant hoher IT-Security – unabhängig
  von Ihren internen Personalressourcen
- Machen Sie sich unsere Projekt- und Branchenerfahrung zunutze – egal, ob Sie Ihre IT bisher in Eigenregie realisiert haben oder bereits Cloud-Anwendungen nutzen
- Unser Angebot umfasst sowohl standardisierte Pakete zu aktuellen Securtiy-Themen als auch hochindividuelles Consulting



Magenta security
It-Sicherheit für den mittelstand

360⁰ IT-Sicherheit aus der Cloud oder beim Kunden vor Ort

	Sicherheits-beratung	Sicherheit für Netzwerke und Infrastruktur	Sicherheit für Endgeräte und Zusammenarbeit	Sicherheit für Identitäten und Zugänge	Sicherheit bei neuen Angriffsmustern
Für jeden Baustein bietet Telekom Technologien de jeweils besten Hersteller im Markt, kombiniert mit eigenen Service- und Betriebs-leistungen	▪ Strategische Beratung ▪ Technologie- und Prozess-beratung	▪ Firewall (auch nächste Generation) für LAN ▪ Antivirus für LAN ▪ Mailverkehr absichern ▪ Webanwendungen sicher nutzen ▪ Industrieanlagen sichern ▪ Massenangriffe (DDoS) verhindern	▪ Firewall für Endgeräte ▪ Antivirus für Endgeräte ▪ Schnittstellen sichern ▪ Verschlüsselung von Daten ▪ Sicheres Arbeiten	▪ Mailinhalte verschlüsseln ▪ Sicherer Zugang zu Cloud-Anwendungen ▪ Passwort-Sicherheit	▪ Anomalien im Datenverkehr aufspüren ▪ Schwachstellen aufdecken ▪ Forensische Soforthilfe
	Dienstleistungen für Konfiguration und Implementierung sowie Betrieb und proaktives Management aus dem Telekom Security Operation Center (SOC)				

security Consulting
Unser angebot im überblick

Bestseller

Consulting Themen	Kurzbeschreibung
Orientierungsworkshop	Sicherheitsworkshop analysiert Ihre IT Infrastruktur: Netzwerke, Endgeräte, Applikationen, etc.
Penetrationtests	Penetrationstests können für Netzwerke und Applikationen durchgeführt werden
EU-Datenschutzgrundverordnung	Workshop zur strukturierten Umsetzung der EU-DSGVO
ISMS Vertiefung	ISMS Workshop vertieft ein vom Kunden gewähltes Thema (z.B. ISMS-Bereiche, Risikomanagement)
Umstellung auf All-IP	Workshop zu den Sicherheitsaspekten der All-IP Technologie
Security Checkup	Analyse der Bedrohungssituation in Unternehmen mit Hilfe einer Check Point Appliance
Mitarbeitersensibilisierung	Workshop zur Definition von Sensibilisierungsmaßnahmen
Netzwerksicherheit	Workshop zur Netzwerksicherheit, Hybride Netzwerke (MPLS vs. Internet), Internetzugang
NG Firewall	Vorteile von Firewalls der nächsten Generation; Einschätzung der Migrationsfähigkeit
Schutz vor DDoS Angriffen	Workshop zu DDoS (Allgemeines, Situation des Kunden, Empfehlungen)
Clouds sicher nutzen	Illustration Cloud-Sicherheit, Migrationswege in Clouds und Cloud-(Sicherheits)-Dienste
Sicherheit mobiler Endgeräte	Workshop zu Trends & Lösungen, Diskussion der Kundensituation, Empfehlungen
APT Strategie & Roadmap	APT Vertiefung (inkl. Interviews); Definition einer APT Schutzstrategie & Roadmap
CERT & Incident Response Management	Workshop zur Vertiefung CERT & Vorfallmanagement; Maßnahmenbedarfsanalyse

Besondere Anforderungen? Sprechen Sie uns!

Orientierungsworkshop
Erfassen Sie Ihre Situation

Ihre AusgangsLage

- Historisch gewachsene IT-Umgebung mit diversen, technischen Sicherheitskomponenten
- Komplexe und anspruchsvolle Sicherheitsarchitektur
- Klassische IT-Sicherheit ohne Berücksichtigung von aktuellen Angriffsmustern (z. B. zielgerichtete Angriffe)
- Umfassender Analysebedarf zum Schutzniveau und zum bestehenden IT-Sicherheitskonzept

Ihre konkreten Fragen

- Auf welchem Sicherheitsniveau befinden wir uns?
- Besonderer Schutzbedarf für welche Unternehmenswerte?
- Welche Sicherheitsmaßnahmen nutzen wir bereits?
- Wo muss bzw. soll unsere IT-Sicherheit in Zukunft stehen?
  - Habe ich alle relevanten Bereiche wie Netzwerk, Clients, Applikationen etc. in meinem

Ihr nutzen

- Individueller Workshop zur Analyse Ihrer IT-Infrastruktur: Netzwerk, Clients, Anwendungen, Authentifizierung und Nutzerverwaltung, Rechtemanagement und betriebliche Anforderungen
- Lösungsvorschlag auf Basis der Ergebnisse und der Risikoanalyse Ihrer Geschäftsprozesse
- Präsentation inklusive Handlungsempfehlungen

Ihre Vorteile

- Klare Orientierung, wo Ihre IT-Sicherheit heute steht –
  und wo Sie hinwollen
- Ganzheitliche Betrachtung Ihrer Infrastruktur
- Know-how aus über 25 Jahre Projekterfahrung
- Zertifizierte Sicherheitsberater bundesweit
- Herstellerneutrale Empfehlungen

Zur Übersicht

PenetrationsTests
Denken wie der Angreifer

Ihre AusgangsLage

- Angreifer sind technisch versiert, extrem flexibel und nutzen jede erdenkliche Schwachstelle aus
- Angreifer haben die unterschiedlichsten Motive, von Geldgier bis politische Ziele
- Jede Organisation kann und wird ein Angriffsziel sein!
- Nachbilden realer Angriffe gegen Netzwerke, Systeme und Applikationen (z. B. basierend auf OWASP)

Ihre konkreten Fragen

Sind Angreifer in der Lage

- die Kontrolle über Ihre Netzwerke zu übernehmen?
- ausrangierte oder unbekannte Systeme auszunutzen?
- interne Dienste zu missbrauchen?
- geschäftskritische Web-Applikationen zu kontrollieren?
- auf geschäftskritische Daten zuzugreifen?

Ihr Nutzen

- So tief eindringen wie möglich und abgestimmt
- Reduktion des Schadensrisikos auf akzeptables Niveau
- Abschlussbericht mit identifizierten Sicherheitslücken und detaillierten Empfehlungen von Gegenmaßnahmen
- Präsentation einschl. Handlungsempfehlungen

Ihre Vorteile

- Ergebnisse helfen, Verbesserungen und Bereinigungen zu koordinieren
- Weitreichendes Expertenwissen zu allen relevanten, technischen Aspekten; mehr als 20-jährige Erfahrung
- Penetrationstests stehen im Einklang mit den aktuellen, vorbildlichen Verfahren
- Unvoreingenommene Sichtweise eines Dritten

Zur Übersicht

EU-DSGVO
DER DSGVO GUT VORBEREITET ENTGEGENSEHEN

Ihre AusgangsLage

- Am 25. Mai 2018 wird die Datenschutzgrundverordnung (DSGVO) in allen Mitgliedstaaten geltendes Recht. Sie wird in Deutschland das Bundesdatenschutzgesetz (BDSG) ablösen und gilt unmittelbar wie nationales Recht.
- Unternehmen aller Größen und Branchen, die in der EU an-sässig sind oder auch nur Daten von EU-Bürgern ver-arbeiten, müssen sich an die Anforderungen der DSGVO halten.
- Sie fragen sich nun, ob Sie der DSGVO unterliegen und ob in Ihrem Unternehmen die notwendigen Schritte eingeleitet wurden, um die Umsetzung zu gewährleisten.

Ihre konkreten Fragen

- Welche Prozesse/Strukturen müssen angepasst werden?
- Welche Informationspflichten müssen eingeführt werden?
- Welche Rechte haben die Betroffenen und welche Löschkonzepte sind möglich?
- Muss ich meine Datenschutzorganisation anpassen?
- Kann ich einen ext. Datenschutzbeauftragten bestellen?
- Welche Verfahren müssen etabliert werden, um Datenpannen zu erkennen?
- Muss ich die Verträge mit Dienstleistern anpassen?
- Welche datenschutzrelevanten Dokumente muss ich anpassen?

Kundennutzen

- Qualifizierter Überblick über die Neuheiten im Datenschutzrecht
- Transparenz über bestehende Prozesse und notwendige Anpassungen im Hinblick auf die DSGVO (Gap-Analyse)

Ihre Vorteile

- Unterstützung bei der Findung von praxisorientierten und wirtschaftlich sinnvollen Lösungen
- Anleitung, um Risiken aufgrund der DSGVO zu vermeiden möglichen Schadensfällen vorzubeugen

ISMS Vertiefung
Internationaler Standard für Unternehmen

Ihre AusgangsLage

- Informationssicherheit ist bereits ein wichtiger Aspekt im gesamten Unternehmen, wird aber in den unterschiedlichen Bereichen eigenständig gehandhabt
- Das Sicherheitsinformationsmanagement in Ihrem Unternehmen soll künftig an international anerkannten Standards ausgerichtet werden (z. B. ISO2700x)
- Geschäftspartner und Kunden sind international

Ihre konkreten Fragen

- Ist meine Sicherheitsorganisation angemessen?
- Entsprechen meine Dokumentationen den heutigen Anforderungen an ein Managementsystem für Informationssicherheit (ISMS)?
- Welches Optimierungspotential besitzt mein ISMS?
- Meine Kunden erwarten ISO-Zertifizierungen von mir. Was ist der erste Schritt dorthin?

Ihr nutzen

- Ist-Analyse auf Basis von Interviews und Dokumenten
- Bewertung und Soll-Ist-Abgleich
- Dokumentation und Präsentation einschl. Handlungsempfehlungen

Ihre Vorteile

- Ganzheitliche Sicht auf alle Phasen des Lebenszyklus eines ISMS
- Transparenz über das Sicherheitsniveau basierend auf internationalen Standards, z. B. ISO 2700x
- Positive Vertrauenseffekte bei Ihren Kunden
- Zertifizierte Experten garantieren Qualität

Zur Übersicht

umstellung auf ALL-IP
Integration und Schutz

Ihre AusgangsLage

- Mit All IP werden Daten und Sprache über ein gemeinsames Netzwerk übertragen
- Das Netzwerk wird durch den All IP Anschluss flexibler, kann aber auch von neuen Bedrohungen gefährdet sein
- Mit Einsatz der neuen All IP Produkte sollte auch das Sicherheitskonzept auf die geänderten Anforderungen für Sprache und Daten angepasst werden.

Ihre konkreten Fragen

- Wie ändert sich die Situation mit Einsatz von All IP bei mir?
- Muss ich mein Securitykonzept für VoIP und das bestehende IT-Netzwerk anpassen?
- Wie nutze ich die neuen Möglichkeiten mit All IP ohne Angriffstore zu öffnen?
- Wie sichere ich beide Infrastrukturen (Sprache und Daten) gegen Angriffe ab?
- Sie verstehen welche Änderungen mit All IP einher gehen.

Kundennutzen

- Sicherheitsworkshop zur Erörterung der neuen Chancen und Gefahren mit Einsatz All IP
- Individuelle Sicherheitsbewertung – vor der Implementierung von All IP
- Abklären von erforderlichen Sicherheitsmaßnahmen
- Präsentation von Handlungsempfehlungen und Optionen (tiefergehende Beratungspakete können in der Folge zugebucht werden, z.B.: Pentests, etc.)

Ihre Vorteile

- VoIP und Datenverkehr werden gemeinsam betrachtet und potentielle Sicherheitslücken aufgezeigt
- Technisch orientierter Workshop mit konkreten Handlungsempfehlungen
- Profitieren Sie vom Fachwissen eines der führenden, integrierten Telekommunikationsunternehmen weltweit

Zur Übersicht

Security Checkup
analyse zur Bedrohungssituation

Ihre AusgangsLage

- Ihr Unternehmensnetzwerk bietet Zugriff auf wertvolle und geschäftskritische Informationen. Diese Informationen sollten auf keinen Fall in die falschen Hände gelangen.
- Eine frühzeitige Erkennung von verborgenen Bedrohungen ermöglicht es, dass Sie diese Risiken unmittelbar adressieren und Ihr Sicherheitsniveau erhöhen können.

Ihre konkreten Fragen

- Kann ich sicher sein, dass uns böse Überraschungen, die wertvolle Informationen gefährden könnten, erspart bleiben?
- Wie bekomme ich Klarheit, dass keine Malware, Hintertüren, Datenverluste oder andere Sicherheitsschwachstellen vorliegen?

Kundennutzen

- Der Security Checkup bietet eine schnelle und einfach zu implementierende Analyse des Netzwerkverkehrs.
- Die Ergebnisse der Analyse und das damit verbundene Lagebild der Netzwerksicherheit wird in einem Report zusammengefasst, der wertvolle Informationen für das Unternehmen bietet.

Ihre Vorteile

- Analyse des Netzwerktraffics mithilfe einer Check Point Firewall Appliance
- Platzierung in vordefinierte Netz-Bereiche des Kunden
- Durchführungszeitraum 14 Tage
- Ergebnis ist ein detailierter Report, der dem Kunden in einem Ergebnisworkshop vorgestellt wird.
- Herstellerneutral

Zur Übersicht

Mitarbeitersensibilisierung auffälligkeiten erkennen und richtig reagieren

Ihre AusgangsLage

- Mitarbeitersensibilisierung ist der Schlüssel für eine erfolgreiche Integration von Sicherheit in Ihre Organisation
- Menschliches Versagen oder Fehlverhalten ist ein wesentliches IT-Sicherheitsrisiko
- Viele Mitarbeiter kennen ihre wichtige Rolle in der IT-Sicherheit nicht
- Sie müssen zur Informationssicherheit und zum richtigen Reagieren in kritischen Situationen geschult

Ihre konkreten Fragen

- Was sind die Grundbegriffe der Informationssicherheit?
- Wie können meine Mitarbeiter im Arbeitsalltag zur Informationssicherheit beitragen?
- Welche Maßnahmen können sofort das Sicherheitsniveau erhöhen?

Ihr nutzen

- Ganztagesworkshop vor Ort
- Diskussion mit den Teilnehmern
- Abwechslungsreiche Gestaltung der Schulung
- Beispiele aus der Praxis
- Teilnehmerzertifikat mit optionalem Abschlusswissenstest

Ihre Vorteile

- Sensibilisierung der Teilnehmer legt die Basis für ein angemessenes Sicherheitsbewusstsein
- Praxisorientierte Wissensvermittlung schafft Bewusstsein
- Schulungsinhalte werden auf Ihre speziellen Bedürfnisse zugeschnitten

Zur Übersicht

Netzwerksicherheit
Profitieren Sie von Vorteilen hybrider Netzwerke

Ihre AusgangsLage

- Streng abgeschottete Firmennetze, wie seit Jahrzehnten verwendet, werden offener
- Traditionelle Abschottungsmaßnahmen bröckeln. WLAN, 4G / 5G, und Cloud-Dienste prägen heute die Arbeitswelt
- Sie möchten Ihr sicheres, privates Netzwerk um kosteneffiziente, öffentliche Netzwerke erweitern und lokale Netze, öffentliche oder private Cloud-Dienste anbinden etc.

Ihre konkreten Fragen

- Wie kann ich lokale Netze über das Internet anbinden?
- Wie gestalte ich Netzwerkübergänge für lokale Netze? Wie kann ich hierzu Cloud-Sicherheitsdienste einsetzen?
- Kann ich einen Hybridansatz verwenden?
- In welchen Fällen kann ich öffentliche Netzwerke verwenden?

Ihr nutzen

- Individueller Workshop analysiert Ihr technisches Design und identifiziert Ihren Bedarf
- Ermitteln von Lösungen für die sichere Anbindung lokaler Netze und Standorte
- Identifikation notwendiger Anpassungen des Ist-Zustands
- Präsentation inklusive Handlungsempfehlungen

Ihre Vorteile

- Optimale Vorbereitung zur langfristigen Absicherung Ihrer Netzwerke
- Technisch orientierter Workshop mit konkreten, individuellen Empfehlungen
- Sicherheitsexpertise aus über 25 Jahren Erfahrung
- Profitieren Sie vom Fachwissen eines der führenden, integrierten Telekommunikationsunternehmen weltweit

Zur Übersicht

NG Firewall
Sichern und Vereinfachen Sie Ihr Geschäft

Ihre AusgangsLage

- Streng abgeschottete Firmennetze, wie seit Jahrzehnten verwendet, werden offener
- Wirkungsschwache Sicherheitslösungen, komplexes Management, teuer, dürftiges Endnutzererlebnis
- Sie streben eine Modernisierung Ihres Internetzugangs an und wollen Schutz vor Cyberattacken

Ihre konkreten Fragen

- Wie kann ich mein Geschäft gegen neue Bedrohungen schützen?
- Wie viele verschiedene Sicherheitssysteme verwende ich?
- Wie kann ich die IT-Kosten unter Kontrolle halten?
- Wie kann ich meine Sicherheitsrichtlinien durchsetzen?
- Bin ich vorbereitet, um zu einer Firewalllösung der

Ihr nutzen

- Individueller Workshop analysiert Ihre Netzwerk- und Sicherheitsumgebung
- Möglichkeiten prüfen, die existierenden Sicherheits-lösungen, z. B. Websicherheit, durch schlagkräftigere Lösungen zu ersetzen
- Prüfe Reifegrad für Migration. Optional: Proof of Concept
- Präsentation mit Handlungsempfehlungen

Ihre Vorteile

- Erfahrung und Fachwissen bei der Planung, dem Aufbau und dem Betrieb von Firewalls der nächsten Generation
- Sicherheitsexpertise aus über 25 Jahren Erfahrung
- Profitieren Sie vom Fachwissen eines der führenden, integrierten Telekommunikationsunternehmen weltweit

Zur Übersicht

Schutz vor DDOS-Angriffen
Schützen Sie Sich vor massiven Angriffen

Ihre AusgangsLage

- Geschäftsprozesse sind heute in hohem Maße von der Verfügbarkeit von Online-Diensten abhängig
- Der Ausfall dieser Online-Dienste kann zu erheblichen Kosten und Imageverlust führen
- DDoS-Angriffe sind mittlerweile ein zentrales Instrument des Geschäfts von Cyberkriminellen
- Volumenangriffe, Angriffe auf Applikationen, Angriffe auf Web-Server

Ihre konkreten Fragen

- Welche Schutzmechanismen gegen DDoS-Angriffe gibt es?
- Welche Bereiche meines Netzwerks / meiner Services sind bereits gut geschützt?
- Gibt es Schwachstellen und folglich Angriffsziele?
- Wo fehlt effektiver Schutz?
- Was sollte ich tun, um mein Netzwerk / meine Dienste gegen DDoS-Angriffe zu schützen?

- Kundenspezifischer Workshop mit Analyse des Netzwerks, der Applikationen und Web-Dienste hinsichtlich des Schutzes vor DDoS-Angriffen
- Übersicht der Netzwerkinfrastruktur, des Internetverkehrs und IP-basierter Applikationen
- Lösung basierend auf den Ergebnissen und der Risikoanalyse Ihrer Geschäftsprozesse
- Präsentation mit Handlungsempfehlungen

Ihr nutzen

- Kundenspezifischer Workshop mit konkreten technischen und organisatorischen Empfehlungen zur Absicherung gegen DDoS Attacken
- Absicherung gegen jedes bekannte DDoS-Szenario durch die drei DDoS-Defence Bausteine der Telekom: Backbone-, on-Premises- und Cloud-Web- DDoS-Protection.

Ihre Vorteile

Zur Übersicht

Clouds sicher nutzen
Profitieren Sie von Clouds

Ihre AusgangsLage

- Sie überlegen, Ihre traditionelle IT in die Cloud zu bringen oder zumindest einige ICT-(Sicherheits)-Dienste aus der Cloud heraus zu nutzen
- Sie möchten die Sicherheitsaspekte beim Übergang in die Cloud verstehen
- Oder Sie nutzen bereits Cloud-Dienste in unterschiedlichen Formen (Private / Public Cloud) und möchten Ihre IT-Security entsprechend anpassen

Ihre konkreten Fragen

- Wie wird Sicherheit üblicherweise in Clouds integriert?
- Was bedeutet ein Wechsel in die Cloud für meine Sicherheit und wie könnte ein sicherer Wechsel aussehen?
- Wie kann ich mir (Sicherheits)-Dienste aus der Cloud zunutze machen?
- Welche Risiken bleiben, wenn ich Cloud-Dienste verwende, im Vergleich zu meinem derzeitigen Betriebsmodell?

Ihr nutzen

- Basierend auf Workshops
- Einführung in die Cloud-Sicherheit und der generelle Einfluss von Cloud-Diensten
- Beantwortung Ihrer Fragen zum Übergang in die Cloud oder bei Verwendung von Cloud-(Sicherheits)-Diensten in Ihrer aktuellen Situation
- Präsentation einschließlich Handlungsempfehlungen

Ihre Vorteile

- Verständnis der Cloud-Sicherheit und was es für Sie bedeutet, wenn Sie Cloud-(Sicherheits)-Dienste nutzen
- Workshop-basierter Ansatz stellt sicher, dass Ihre konkreten Fragen beantwortet werden und Sie am Ende individuelle Empfehlungen erhalten
- Profitieren Sie von unseren zahlreichen, erfolgreichen Übergängen in Clouds für große und

Zur Übersicht

Sicherheit mobiler Endgeräte
Nutzen Sie die Vorteile Mobiler Endgeräte

Ihre AusgangsLage

- Heutige Geschäftsabläufe profitieren mehr und mehr von mobilen Endgeräten. Diese Geräte gestatten Zugriff auf geschäftskritische Daten.
- Die sichere Integration von mobilen Endgeräten in Ihre Geschäftsprozesse und ICT-Infrastruktur ist essentiell für den Schutz Ihres wertvollen Firmeneigentums
- Sie wollen die Sicherheitsfragen bei der Verwendung mobiler Endgeräte verstehen

Ihre konkreten Fragen

- Wie kann ich mobile Endgeräte sicher in meine ICT-Infrastruktur integrieren?
- Welche Arten von Sicherheitsdiensten, z. B. Authentisieren, Verschlüsseln, Anti-Virus, sollte ich nutzen?
- Wie kann ich mich vor fortgeschrittenen Angriffen gegen meine mobilen Endgeräte schützen?
- Bedeutet BYOD zusätzliche Sicherheitsrisiken?

Workshop-basierter Ansatz

- Einführung in die Sicherheit mobiler Endgeräte
- Beurteilung der Kundensituation, insbesondere heutige Risiken
- Vorschlag für eine maßgeschneiderte Herangehensweise an das Thema „Mobile Sicherheit“
- Präsentation einschließlich Empfehlungen nächster Schritte

Ihr nutzen

- Verstehen Sie die heutigen Risiken beim Einsatz von mobilen Endgeräten
- Entwickeln Sie eine Vorstellung, wie sie in Zukunft mobile Endgeräte schützen können
- Profitieren Sie vom Fachwissen eines der führenden, integrierten Telekommunikationsunternehmen weltweit

Ihre Vorteile

Zur Übersicht

APT Strategie & Roadmap
Seien Sie Vorbereitet auf APT-Angriffe

Ihre AusgangsLage

- Cyber-Kriminelle werden immer professioneller
- Angreifer verweilen unbemerkt für mehr als 200 Tage in Netzwerken und Systemen und haben dabei schier unbegrenzte Möglichkeiten, Schaden anzurichten
- Komplexe und schwierige Sicherheitsarchitektur
- Traditionelle IT-Sicherheit, ohne aktuelle Angriffsmuster (APT=Advanced Persistent Threat) zu berücksichtigen

Ihre konkreten Fragen

- Welche Sicherheitsmaßnahmen sind erforderlich, um besser auf APT-Angriffe vorbereitet zu sein?
- Welche Ergänzungen unserer IT-Sicherheit sind in naher Zukunft notwendig?
- Wie kann ich APT-Abwehrmaßnahmen in meine Geschäftsstrategie integrieren?
- Kann ich mit Managed SOC Services meinen Schutz verbessern?

Ihr nutzen

- Individueller Workshop analysiert Ihre IT-Infrastruktur und Reifegrad bzgl. APT, einschl. technischer Lösungen, Menschen und Mitarbeiter, Prozesse, mit einem Fokus auf technischen Lösungen
- Dokumentierte Strategie und Roadmap hin zu APT-Stärke
- Ergebnispräsentation

Ihre Vorteile

- Klare Orientierung, wo Sie beim Thema „APT“ stehen bzgl. Menschen und Mitarbeiter, Prozesse und technische Lösungen sowie Empfehlungen zukünftiger Schritte
- Fachexperten zu allen relevanten, technischen Aspekten
- Unvoreingenommene Sicht eines Dritten, der seit langer Zeit eigene Cyber Defense Center und SOCs

Zur Übersicht

Cert & Incident response management
Verstehen wie MAN CERT & IRM organisiert

Ihre AusgangsLage

- Die heftig gestiegene Zahl von Cyber-Angriffen gegen Firmen aller Bereiche macht es mehr als wahrscheinlich, dass auch Sie Opfer einer Cyber-Attacke werden
- Adäquate Vorbereitung ist der Schlüssel, um die Auswirkungen von Angriffen zu reduzieren
- Sie müssen Ihr vorhandenes CERT & Incident Response (Vorfallsmanagement) erweitern oder sind sich schlicht im Unklaren, wo Sie gegenwärtig stehen

Ihre konkreten Fragen

- Bin ich gut vorbereitet, Sicherheitsvorfälle zu entdecken?
- Sind meine Verantwortlichkeiten wohldefiniert?
- Sind meine Prozesse und technische Infrastruktur adäquat oder wo müssen diese verbessert werden?
- Brauche ich mein eigenes CERT?
  - Wie kann ich Dienste Dritter einsetzen, insbesondere bei kritischen Situationen?

Ihr nutzen

- Workshop-basierter Ansatz
- Verständnis der Aufgaben eines CERT & IR Managements
- Überprüfung des vorhandenen CERT & IR Managements (Vorfallsentdeckung und -klassifizierung, IRM Prozesse, Mitarbeiter, technische Fähigkeiten, Eskalationsprozesse)
- Definition geeigneter CERT & IRM Funktionen
- Präsentation einschl. Empfehlungen nächster Schritte

Ihre Vorteile

- Verstehen Sie, warum CERT & IRM essentiell für den Schutz Ihrer Geschäfte sind
- Lernen Sie, eine geeignete Organisation und passende Prozesse aufzubauen und wie Sie unterstützende Dienste einsetzen können
- Profitieren Sie von der langjährigen Erfahrung der DTAG, des TSI CERT, des dCERT und unserer IRM Praxiskenntnis

Zur Übersicht

security Consulting
Unser angebot im überblick

Consulting Themen	Preis **ab**
Orientierungsworkshop je nach Komplexität der IT	4.900 Euro / 2.969 Euro
Penetrationtests	Netzwerk oder Applikation ab 6.500 Euro / APT ab 9.000 Euro
EU-Datenschutzgrundverordnung	2.675 Euro
ISMS Vertiefung	6.000 Euro
Umstellung auf All-IP	2.900 Euro
Security Checkup	3.900 Euro
Mitarbeitersensibilisierung	2.350 Euro
Netzwerksicherheit	4.600 Euro
NG Firewall	2.900 Euro
Schutz vor DDoS Angriffen	3.500 Euro
Clouds sicher nutzen	5.300 Euro
Sicherheit mobiler Endgeräte	4.000 Euro
APT Strategie & Roadmap	12.500 Euro
CERT & Incident Response Management	4.000 Euro

Besondere Anforderungen? Sprechen Sie uns an.