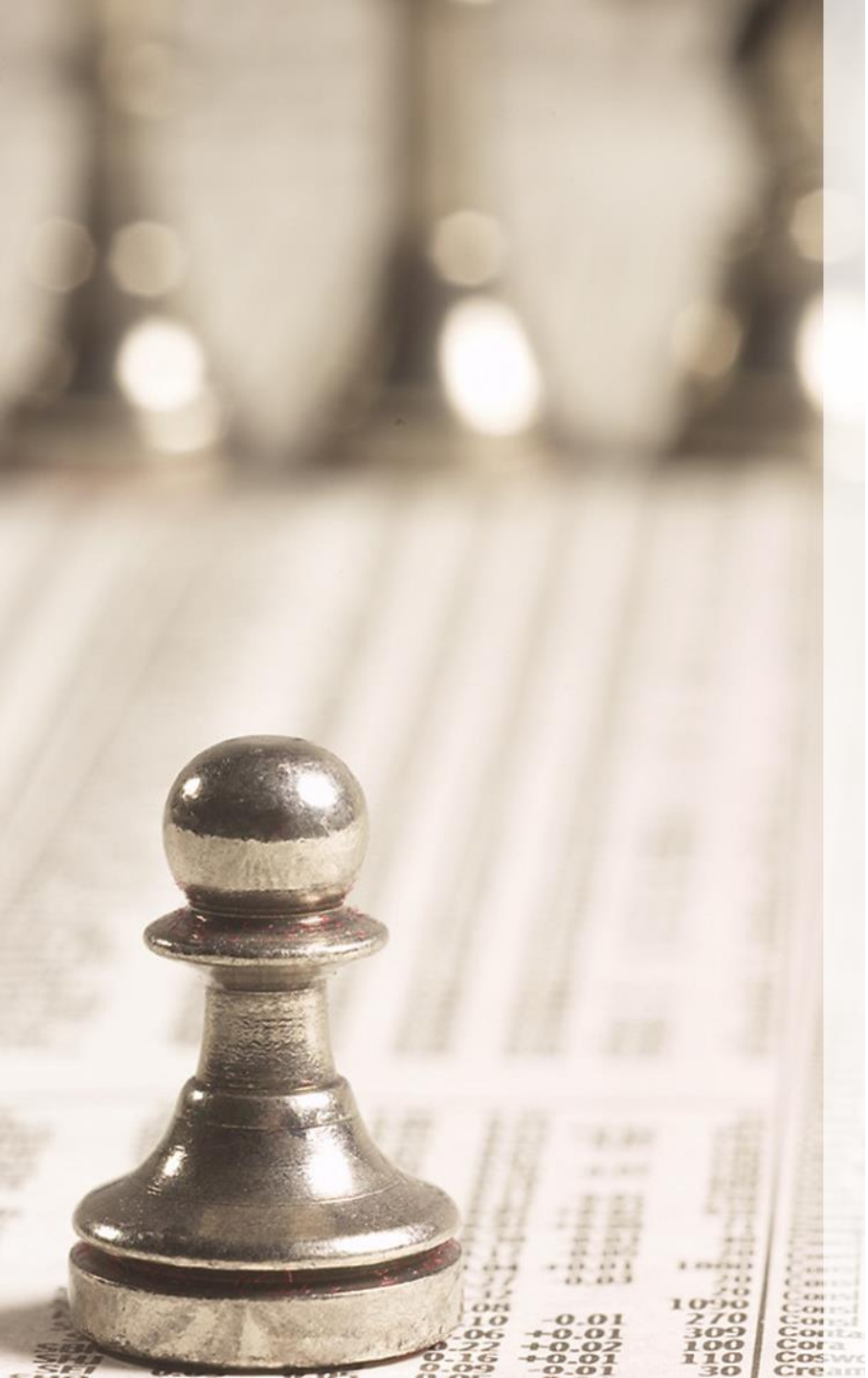

Quick Check zur IT-Sicherheit

Transparenz über technische und organisatorische Sicherheitslücken schaffen

DEUTSCHE GESELLSCHAFT FÜR
CYBERSICHERHEIT mbH & Co. KG

arf

Agenda

Unternehmensdarstellung
Deutsche Gesellschaft für Cybersicherheit

DEUTSCHE GESELLSCHAFT FÜR
CYBERSICHERHEIT mbH & Co. KG

- Die „Deutsche Gesellschaft für Cybersicherheit mbH & Co. KG“ ist ein international tätiges, unabhängiges und durch den alleinigen geschäftsführenden Gesellschafter Matthias Nehls geführtes Unternehmen mit Sitz in Schuby bei Schleswig, im Norden Deutschlands.
- Wir testen und analysieren die IT-Systeme unserer Kunden, verbunden mit dem Ziel, deren IT-Strukturen vor potentiellen Hacker-Angriffen zu schützen. Dabei decken wir Sicherheitslücken auf und helfen unseren Kunden diese zu beseitigen.
- Es gehört zu unserem Selbstverständnis, unsere Kunden persönlich, unabhängig und mit einem Höchstmaß an Objektivität und Neutralität zu beraten.

Unternehmensdarstellung
arf GmbH

- Die arf GmbH gründete sich aus der LGA Landesgewerbeanstalt Bayern (Körperschaft des öffentlichen Rechts, gegründet im Jahr 1869).
- Im GJ 2016/2017 ca. 40 Mitarbeiter/innen und ein umfangreiches Netzwerk von freiberuflichen Experten und Kooperationspartnern, die projektspezifisch eingesetzt werden.
- Seit mehr als 20 Jahren konzentrieren wir uns auf Problemstellungen und Lösungsansätze für den öffentlichen Dienst.
- In unseren Kompetenzbereichen verfügen unsere Beratungsteams über umfassende Methoden- und Managementerfahrungen
  - IT und IT-Qualitätssicherung
  - Organisation und Veränderungsmanagement
  - Strategie und Führung
  - Haushalt und Controlling
  - Bilanzierung und Buchhaltung

Agenda

IT-Sicherheit wird zunehmend zu einem wirtschaftlich relevanten Faktor

- Digitalisierung und Vernetzung erhöhen die Abhängigkeit in Wirtschaft und Verwaltung von funktionsfähigen IT-Verfahren. Ein Ausfall der Systeme führt zu relevanten wirtschaftlichen Schäden und Einschränkungen im Leistungsangebot.

- Der Verlust von wirtschaftlich relevanten Daten schränkt die Arbeitsfähigkeit einer Organisation ein und führt zu einem Vertrauensverlust bei BürgerInnen/Kunden.

- Die Nutzung der eigenen IT-Infrastruktur durch Dritte kann neben einem wirtschaftlichen Schaden auch zu (straf-)rechtlich relevanten Fragestellungen führen.

Konkrete Schadensereignisse werden fast täglich bekannt

- Eingeschränkte Verfügbarkeit oder Zerstörung von IT-Infrastruktur
- Zugriff auf schützenswerte Daten oder deren Löschung durch Dritte
- Manipulation von Daten und Auslösung wirtschaftlich und/oder rechtlich relevanter Prozesse (z.B. Buchung von Auszahlungsbelegen)
- Übernahme der Steuerung von relevanter Infrastruktur (z.B. Energieversorgung oder (Produktions-)Maschinen)

Kennen Sie den Status Ihrer IT-Sicherheit?

- Normen aus dem Bereich der IT-Sicherheit (BSI Grundschutz oder ISO 27001) schaffen Bewusstsein für das Thema IT-Sicherheit und verankern Prozesse und Strukturen in der Organisation, die die IT-Sicherheit fördern.
- In der Praxis entsteht dadurch aber nicht zwingend auch eine angemessene Sicherheit, da häufig Prozesse im Detail nicht in geeigneter Form ausgestaltet werden oder bei Mitarbeitern kein ausreichendes Sicherheitsbewusstsein erzeugt werden konnte.

Eine regelmäßige Überprüfung des Gefährdungspotenzials im Bereich der IT ist für jede Organisation zu empfehlen.
Konkrete technische oder organisatorische Schwachstellen können so zeitnah identifiziert und abgestellt werden.

Agenda

Unser Quick Check zur IT-Sicherheit schafft Transparenz über Sicherheitslücken

Penetrationstest	Organisations-Check	Handlungs-empfehlungen	Umsetzung (optional)
▪ Simulation externer Angriffe ▪ Simulation interner Angriffe ▪ Darstellung und Bewertung der Schadenpotenziale/ technischen Schwachstellen	▪ Inhaltliche Lücken im Bereich von Sicher-heitsrichtlinien ▪ Fehlende Konkreti-sierung von Prozessen (z.B. Checklisten) oder Kontrollen ▪ Reifegradbestimmung und Ableitung zu erwartender organisatorischer Schwachstellen ▪ Schulung und Mitarbeiterverhalten	▪ Priorisierung der Sicherheitslücken nach dem Schaden-potenzial ▪ Ausarbeitung technischer und organisatorischer Maßnahmen	▪ Begleitung von Umsetzungsmaß-nahmen ▪ Bewertung von Lösungsansätzen im Bereich der IT-Sicherheit ▪ Vorbereitung von IT-Sicherheits-zertifizierungen

Regelmäßige Wiederholung des Quick Checks zur IT-Sicherheit

Agenda

1 Unternehmensdarstellungen

2 Thematische Einordnung: IT-Sicherheit

3 IT-Sicherheit Quick Check

3.1 **Penetrationstest**

3.2 Organisatorischer Quick Check

3.3 Handlungsempfehlungen

3.4 Umsetzung

Der **Penetrationstest** zeigt das konkret bestehende technische Gefährdungspotenzial auf

- Black-box Angriffsszenario: Simulation eines Hackerangriffs über die Website und die Firewall der Organisation (extern) bzw. zugänglicher Netzinfrastruktur (intern) ohne Vorkenntnis der vorhandenen Infrastruktur. Anwendung von Methoden und Werkzeugen von Cyberkriminellen.

- Aufbereitung der gewonnen Informationen
  - Erreichbare Systeme und deren Konfiguration
  - Steuerbare Systeme
  - Zugriffsmöglichkeiten auf Daten und Anwendungen

- Darstellung der Schadenpotenziale
  - Durch Zugriffsmöglichkeit auf Daten: Entwendung, Manipulation oder Zerstörung von Daten
  - Durch Zugriffsmöglichkeit auf Systeme/Anwendungen: Steuerung, Ausfall oder Zerstörung von Systemen/Systemkomponenten

Agenda

Drei wesentliche Schritte des organisatorischen **Quick Checks**

Neben dem Penetrationstest erfolgt ein organisatorischer und prozessualer Quick Check in unterschiedlichen Schritten

	Reifegradanalyse	Vertiefende Interviews	Identifikation von Schwachstellen
1	Die bestehenden Organisations-strukturen und -prozesse in den relevanten Organisationseinheiten zur IT- Sicherheit werden parallel zum Penetrationstest analysiert	Aufbauend auf der technischen Analyse Ist-Aufnahme in der Organisation werden vertiefende Interviews geführt	Als Resultat der technischen Analyse, der Reifegradbestimmung und der vertiefenden Interviews werden konkrete Schwachstellen beschrieben
2	Der Reifegrad berücksichtigt 1. Wie hoch ist das Sicherheits-bewusstsein der Organisation? 2. Wie ist der Stand der bestehenden **IT-Sicherheitskonzepte**? Entspricht es den aktuellen Anforderungen? 3. Welche **Anforderungsprofile** werden an die Mitarbeitenden gestellt? Werden diese derzeit erfüült?	Folgende Interviewpartner sind dafür vorgesehen: 1. Geschäftsführung 2. Abteilungsleitung der IT 3. Datenschutzbeauftragte/r 4. IT-Sicherheitsbeauftragte/r	Daraus resultieren Handlungsempfehlungen und die Formulierung und Priorisierung konkreter Maßnahmen/ Regelungen Dazu gehören u.a. Hinweise zur Überarbeitung der (bestehenden) IT-Sicherheitsleitlinien und zur Weiterentwicklung von Anforderungs-profilen der MA

Agenda

1 Unternehmensdarstellungen

2 Thematische Einordnung: IT-Sicherheit

3 IT-Sicherheit Quick Check

3.1 Penetrationstest

3.2 Organisatorischer Quick Check

3.3 **Handlungsempfehlungen**

3.4 Umsetzung

Der organisatorische Quick Check geht auf die Ergebnisse des Penetrationstests ein und leitet entsprechende **Handlungsempfehlungen** ab

- Häufig können Sicherheitslücken durch organisatorische Maßnahmen geschlossen werden:
  - Checklisten können helfen, dass bei der Konfiguration der IT-sicherheitsrelevante Einstellungen auch tatsächlich vorgenommen werden
  - Zugangskontrollen und Absicherung von Netzzugangspunkten sowie sicherheitsbewusstes Verhalten der Mitarbeiter können Angriffsrisiken von innen verringern
  - Organisation regelmäßiger Sicherheitsupdates für die eingesetzte Hard- und Software
  - Die identifizierten Sicherheitslücken können durch das Aufsetzen regelmäßiger Kontrollen (Sicherheitsmonitoring) überwacht werden
- Auch können technische Schwachstellen transparent werden, für deren Behebungen Maßnahmen vorgestellt werden.
- Ein Maßnahmenkatalog zeigt insgesamt auf, welche organisatorischen Maßnahmen in der konkreten Situation sinnvoll sind um nachgewiesene Sicherheitslücken zukünftig zu vermeiden.

Agenda

1 Unternehmensdarstellungen

2 Thematische Einordnung: IT-Sicherheit

3 IT-Sicherheit Quick Check

3.1 Penetrationstest

3.2 Organisatorischer Quick Check

3.3 Handlungsempfehlungen

3.4 **Umsetzung**

Umsetzung

- Unser Angebot für die Umsetzung beinhaltet folgende Aspekte:

  - ✓ Unabhängige Begleitung und Qualitätssicherung von Maßnahmen zur Verbesserung der IT-Sicherheit
  - ✓ Unterstützung bei der Erstellung von Richtlinien im Bereich der IT-Sicherheit
  - ✓ Begleitung von Prozessoptimierungen
  - ✓ Durchführung von Qualifizierungsmaßnahmen für Mitarbeitende

Für Fragen stehen wir gerne zur Verfügung!

Dr. Jörg Erdmann

Bereichsleiter IT & IT-Qualitätssicherung

arf Gesellschaft für Organisationsentwicklung mbH

Schiffgraben 25
D-30159 Hannover

Tel.: +49 511 35 37 47 07
Mobil:+49 162 21 21 94 9
Fax: +49 511 35 37 47 08
www.arf-gmbh.de
joerg.erdmann@arf-gmbh.de