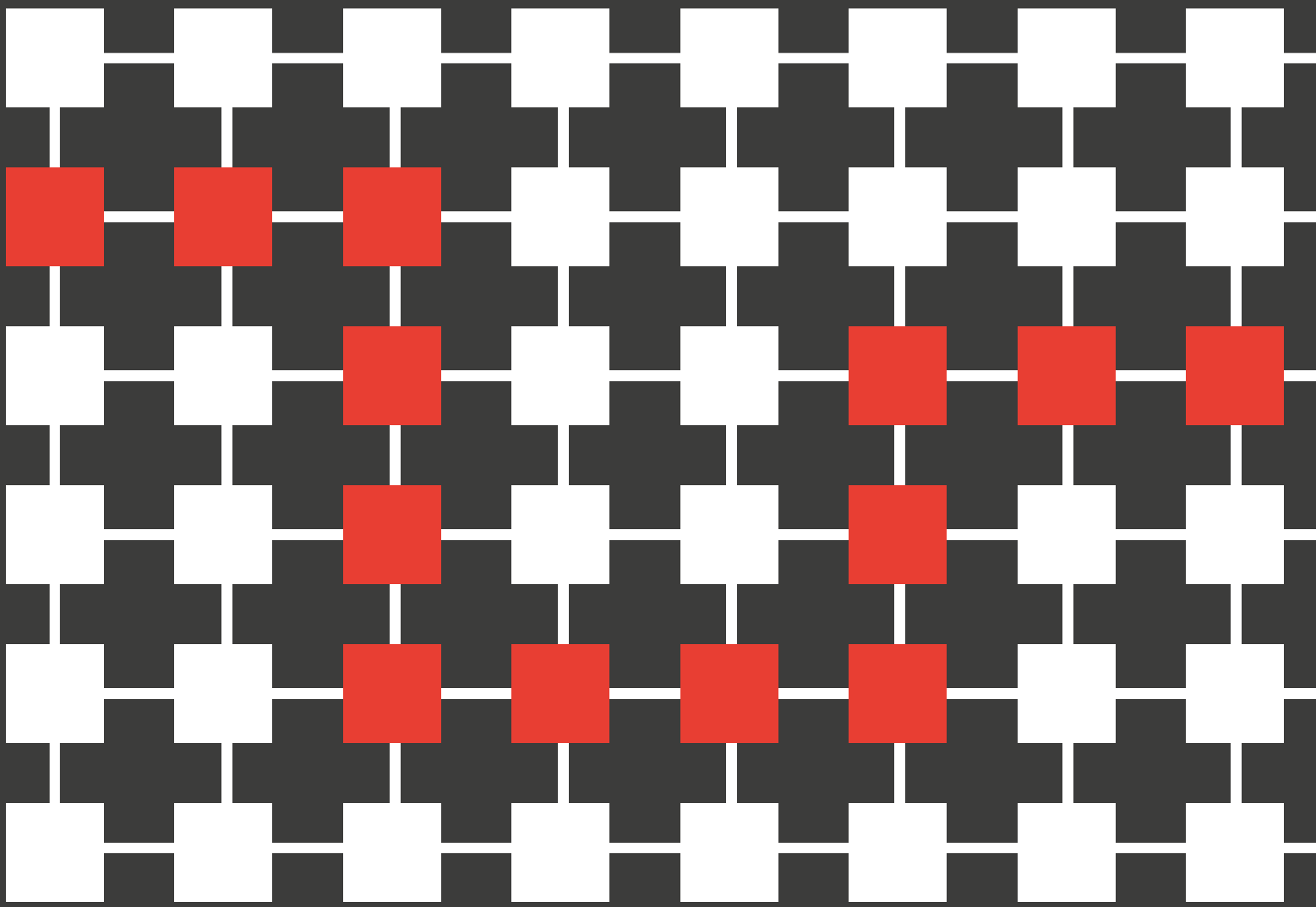
www.pwc.de/cybersecurity

Schutz Kritischer Infrastrukturen angesichts der aktuellen geopolitischen Lage



pwc

Der Schutz Kritischer Infrastrukturen (KRITIS) wird künftig bedeutender denn je – wir unterstützen nationale und internationale Unternehmen sowie die öffentliche Hand bei den anstehenden Herausforderungen

Ernährung
Die Versorgung von Geflüchteten sowie Betroffenen in Krisengebieten, aber auch weltweit, macht den Bereich Ernährung zu einem Angriffsziel. Ein Krisen-Lagebild ist zwingend erforderlich.

IT und Telekommunikation
Störung oder Veränderung von Kommunikation sind Kerninstrumente des Konflikts. IT und Telekommunikation bedürfen besonderen Schutzes, v.a. für 5G/6G.

Ver- und Entsorgung
Insbesondere Energie- und Wasserversorgung dürften in den Fokus rücken. Wir unterstützen bei der Validierung von ISMS und Notfallplänen.

Gesundheit
Krankenhäuser und Maximalversorger rechnen weiter mit Angriffen. Wir begleiten bei Alarm- und Einsatzplanung, Schwachstellenanalysen und vielem mehr.

Transport, Verkehr und Logistik
Transport- und Verkehrsinfrastruktur sehen wir ebenfalls als gefährdet an – im Bereich Logistik sollte ein besonderer Schutz von Dual-Use-Gütern, Ausrüstung u. ä. erfolgen, insbesondere auch durch die weitere Schaffung von Sicherheitsnetzwerken.

Staat und Verwaltung
Bereits vor der aktuellen Krise war eine Aktualisierung des regulatorischen Rahmens dringend notwendig. Dieses Update wird durch die Bundesregierung im Rahmen eines KRITIS Dachgesetzes angestrebt. Wir begleiten Bund und Länder zusammen mit deren Cybereinrichtungen bei dieser Fortentwicklung.

International
Die internationale Zusammenarbeit beim Schutz von KRITIS wird intensiviert. Bei Konzeption und Umsetzung gemeinsamer Maßnahmen unterstützen wir die EU und darüber hinaus.

Finanzen
Banken sind spätestens seit den Sanktionen verstärkt in den Fokus gerückt. Zwar ist die Finanzindustrie einer der am stärksten regulierten Sektoren, doch müssen diese im Rahmen der aktuellen geopolitischen Lage angepasst und erweitert werden.

Unternehmen im besonderen öffentlichen Interesse
Schließlich wird eine gesamtstaatliche Resilienz von überragender Bedeutung sein. Neben dem Schutz wichtiger Unternehmen ist insbesondere eine reibungslose Governance zwischen den Cyber-Behörden des Bundes essentiell.

Cyber Security Experience Center

Wie lässt sich die zunehmende Bedrohung durch Cyberangriffe auf operative Technologien (OT) veranschaulichen – insbesondere in Hinblick auf Kritische Infrastrukturen? Um die hohen Risiken und Herausforderungen in diesem Sektor aufzuzeigen und anschauliche Best Practices für die Erhöhung der IT-Sicherheit zu demonstrieren, betreibt PwC Deutschland in Frankfurt das Cyber Security Experience Center. Hier zeigen Security-Expert:innen, wo operative Technologien wie Industrieroboter, Gasdruckregelanlagen oder Steuerungssysteme (ICS) besonders angreifbar sind. Besuchen Sie uns! Mehr Infos hier: www.pwc.de/cyber-security-experience-center

Die Kritische Infrastruktur ist durch die Nutzung vernetzter Hardware und die Abhängigkeit von Daten und Softwarelösungen durch potenzielle Angriffe auf ihre IT-Infrastruktur gefährdet. Insbesondere in der aktuellen geopolitischen Situation stellen solche „digitalen“ Vergeltungsschläge eine erhöhte Gefahr dar

Warnung an die Bundesregierung

Cyberangriff auf deutsche »Hochwertziele« könnte schon bald starten

In der Regierung steigt die Nervosität wegen möglicher Cyberattacken gegen kritische Infrastruktur. Nach SPIEGEL-Informationen rechnen die Behörden in Kürze mit Angriffen.

07.03.2022, 18.46 Uhr

Quelle: Spiegel Online

Hackerangriffe auf die Ukraine

Die erste Angriffswelle

Die Invasion begann, bevor Raketen einschlugen – mit russischen Hackerattacken. Deren Aktionen beschränken sich nicht auf die Ukraine. Sie können auch den Westen treffen.

Von **Kai Biermann** und **Karsten Polke-Majewski**

24. Februar 2022, 14:45 Uhr / 234 Kommentare

Quelle: zeit Online

KRITISCHE INFRASTRUKTUR SCHÜTZEN

Im Fadenkreuz der Hacker

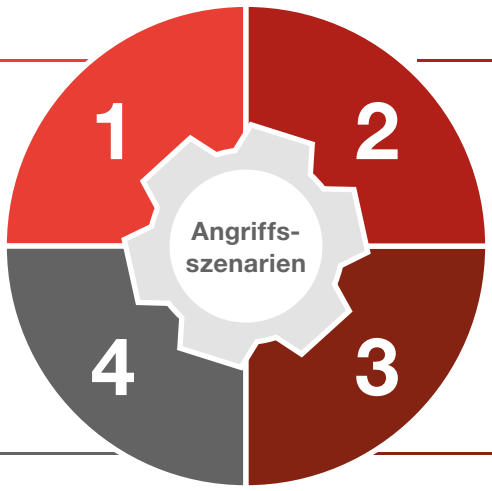
Ein großangelegter Hackerangriff auf Verkehrssysteme oder Kraftwerke, diese Vorstellung macht Angst. Forscher arbeiten daran, mögliche Angriffsziele sicherer zu machen – ein Wettlauf gegen einen unsichtbaren Gegner.

Quelle: Handelsblatt

UKRAINE-RUSSLAND-KONFLIKT

SH ist „mittendrin“ im Cyberkrieg: Es gab Angriffe auf kritische Infrastruktur

Quelle: shz.de



DDOS-Angriffe
Ausfall oder Nicht-Verfügbarkeit notwendiger IT-Systeme, Prozesse und Anwendungen, die zur Erbringung kritischer Dienstleistungen genutzt werden, z. B. Internet-Dienste.

Supply Chain-Angriffe
Angriff auf vorgelagerte Systeme, z. B. Open-Source-Lösungen (Log4J) oder die Systeme eines Zulieferers.

Ransomware-Angriffe
Verschlüsselung oder Veröffentlichung kritischer Informationen und Daten, z. B. digitale Patientenakten.

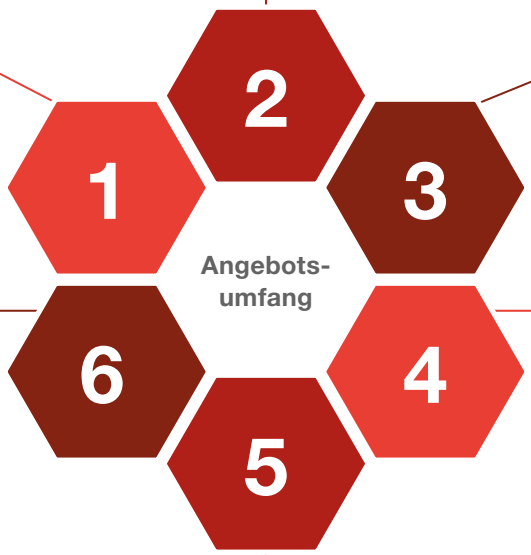
E-Mail-Threats
Nebst Kontrolle über Prozesse, Anwendungen oder IT-Systeme, die zur Erbringung kritischer Dienstleistungen genutzt werden, z. B. APTs.

PwC unterstützt Unternehmen bei der Identifikation schützenswerter Geschäftsprozesse und Betreiber kritischer Geschäftsprozesse bei der Ausarbeitung von Maßnahmen zum sicheren Fortbetrieb bei einem Cyberangriff

Penetrationstests
Evaluierung der Sicherheit der IT-Systeme anhand simulierter Angriffe.

Cyber Maturity Assessment
1-Tages-Workshop zur initialen Bestandsaufnahme der Cybersicherheit einer Institution mit Hilfe des Cyber Security Experience Centers in Frankfurt.

Threat Intelligence
Subscription Service mit zeitlichen, taktischen und strategischen Daten zur aktuellen weltweiten Bedrohungslage im Cyber-Space.



Forensik
Unterstützung bei der Aufarbeitung sowie Untersuchung bei aufgetretenen Cybersicherheitsvorfällen.

Disaster Recovery/ Business Continuity
Analyse des aktuellen Notfallmanagements für kritische Geschäftsprozesse (Game of Threats™). Konzeptionierung und Implementierung von Fallback-Lösungen.

Crisis Management
Interdisziplinäres Krisenmanagement (Incident Response), das Sie bei der Bewältigung von IT-Sicherheitsvorfällen nicht nur im Cyber-Space, sondern über die gesamte Organisation hinweg unterstützt.

PwC begleitet Betreiber Kritischer Infrastrukturen, Regulatoren und Behörden auch bei strategischen, organisatorischen und regulatorischen Fragestellungen im Zusammenhang mit der aktuellen Bedrohungslage

	KRITIS-Betreiber	Regulatoren	Behörden
	• Ist die Institution Betreiber Kritischer Infrastruktur? • Wie sieht die Governance aus? • Ist die Governance der neuen Gefahrenlage gewachsen? • Werden Synergiepotenziale aus möglichen Kooperationen der Unternehmen untereinander ausgeschöpft?	• Wo müssen Regulatoren jetzt eingreifen? • Bedarf es einer krisenadjustierten Ergänzung der Gesetzgebung? • Welche Initiativen sollten strategisch auf der Ebene von Bund und Länder, welche auf EU-Ebene erfolgen?	• Bestehen ausreichend Standards für die Krisen-Angriffsszenarien aus Sicht der Betroffenen? • Ist die Behörde ausreichend mit Kompetenzen ausgestattet? • Ist das Beratungs- und operative Umsetzungsangebot angemessen?
	• Betroffenheitsanalyse • Governance Quick Check • Implementierung von ad-hoc Richtlinien zur Governance • Begleitung konkreter Kooperationsvorhaben, v.a. im interkommunalen Kontext • Prüfungen oder Prüfungsvorbereitung gem. §8a Abs.3 und Abs.4 BSIG	• Potenzielle Anpassungsnotwendigkeit der aktuellen Rechtslage • Zielbildanalysen • Begleitung bei der Ergänzung vorhandener oder Entwicklung neuer Regularien v.a. Krisenverordnung • Prüfungen gem. §8a Abs.4 KRITIS Verordnung	• Digitale Lagebilder • Begleitung behördlicher Gefahrenfeldanalysen und Ableitung behördlicher Gefahrenabwehrmaßnahmen • Optimierung des Beratungs- und Schulungsangebots

PwC begleitet Betreiber Kritischer Infrastrukturen sowie deren Träger insbesondere auch bei der Absicherung der einschlägigen rechtlichen Rahmenbedingungen hinsichtlich der Gewährleistung der Cybersicherheit

Rechtlicher Rahmen Prävention

- Risikoanalyse hinsichtlich IT-sicherheits-rechtlicher und datenschutzrechtlicher Schwachstellen
- Sicherstellung des Schutzes von Geschäftsgeheimnissen nach den einschlägigen Vorgaben des EU- und nationalen Rechts
- Einführung oder Optimierung eines an Krisen adjustierbares Compliance-Management-Systems

Rechtlicher Rahmen Reaktion

- Rechtssichere Schadensaufnahme und Schadensbegrenzung (v.a. hins. Unternehmensinteresse, öffentlicher Daseinsvorsorge, Datenschutz)
- Rechtssichere Vorbereitung von Kommunikationsmaßnahmen
- Abwehr von Haftungsfällen
- Begleitung bei der Information der zuständigen Ermittlungsbehörden und in der Zusammenarbeit mit diesen.

Rechtlicher Rahmen Grundlagen

Welche **Rechtsgrundlagen** müssen Betreiber Kritischer Infrastrukturen beachten?

IT-Sicherheitsgesetz, Datenschutz-Grundverordnung, Telekommunikationsgesetz, Telemediengesetz, Krankenhausgesetze, Gemeindeordnungen etc.

Incident Response: Seien Sie für den Ernstfall vorbereitet und informieren Sie sich hier, wie wir Sie konkret unterstützen können!

Jetzt mehr erfahren.

PwC bietet dafür ein Netzwerk aus Expert:innen mit interdisziplinärer Expertise für alle KRITIS-Sektoren:

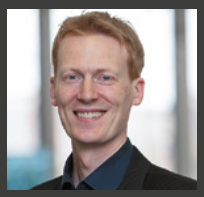
Rainer Bernnat
Partner, Leiter Public Sector,
PwC Strategy&
rainer.bernnat@pwc.com
Tel.: +49 170 2238414

Andre Glenzer
Partner, Leiter KRITIS Center
of Excellence, PwC Deutschland
andre.glenzer@pwc.com
Tel.: +49 160 94470376

Lorenz Kuhlee
Director, Incident Response,
PwC Deutschland
lorenz.kuhlee@pwc.com
Tel.: +49 151 50049769

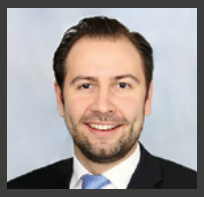
Jörg Asma
Partner, Sektor Gesundheit,
PwC Deutschland
joerg.asma@pwc.com
Tel.: +49 160 6142945

Aleksei Resetko
Partner, Sektor IT & Telekommunikation,
PwC Deutschland
aleksei.resetko@pwc.com
Tel.: +49 151 14268214



Achim Schäfer
Partner, Sektor Finanzen- und
Versicherungswesen, PwC Deutschland
achim.schaefer@pwc.com
Tel.: +49 160 90148201

Johann Hartl
Manager, Sektor UBI, §8a Abs. 4
Prüfungen, PwC Deutschland
johann.hartl@pwc.com
Tel.: +49 151 25913516



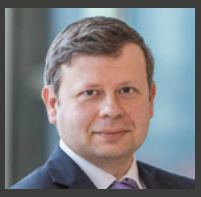
Dr. Nicolas Sonder
Partner, Betroffenheitsanalyse,
PwC Deutschland
nicolas.sonder@de.pwc.com
Tel.: +49 151 52516789

Dr. Oliver Hanka
Director, Leiter Cyber Security
Experience Center Frankfurt,
PwC Deutschland
oliver.hanka@pwc.com
Tel.: +49 160 5105836

Germar Schröder
Partner, Sektor IT & Telekommunikation,
PwC Strategy&
germar.schroeder@pwc.com
Tel.: +49 170 2238426

Karsten Wilop
Partner, Sektor Finanzen- und
Versicherungswesen, PwC Deutschland
karsten.wilop@pwc.com
Tel.:+49 170 5278376

Hendrik Gollnisch
Senior Manager, Sektor Entsorgung,
PwC Deutschland
hendrik.gollnisch@pwc.com
Tel.: +49 170 7862225



Vladyslav Dunajevski
Senior Manager, Sektor
Transport, PwC Deutschland
vladyslav.d.dunajevski@pwc.com
Tel.: +49 151 16953894

Henry Otto
Partner, Sektor Wasser,
PwC Deutschland
henry.otto@pwc.com
Tel.: +49 160 90575374

Derk Fischer
Partner, Sektor Ernährung,
PwC Deutschland
derk.fischer@pwc.com
Tel.: +49 170 7946797

Moritz Anders
Partner, Sektor Energie,
PwC Deutschland
moritz.anders@pwc.com
Tel.: +49 151 55455621

Stephan Vennemann
Senior Manager, Sektor Wasser,
PwC Deutschland
stephan.vennemann@pwc.com
Tel.: +49 160 92526187

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen unseren Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expert:innennetzwerks in 156 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC Deutschland. Über 12.000 engagierte Menschen an 21 Standorten. Knapp 2,4 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.

www.pwc.de