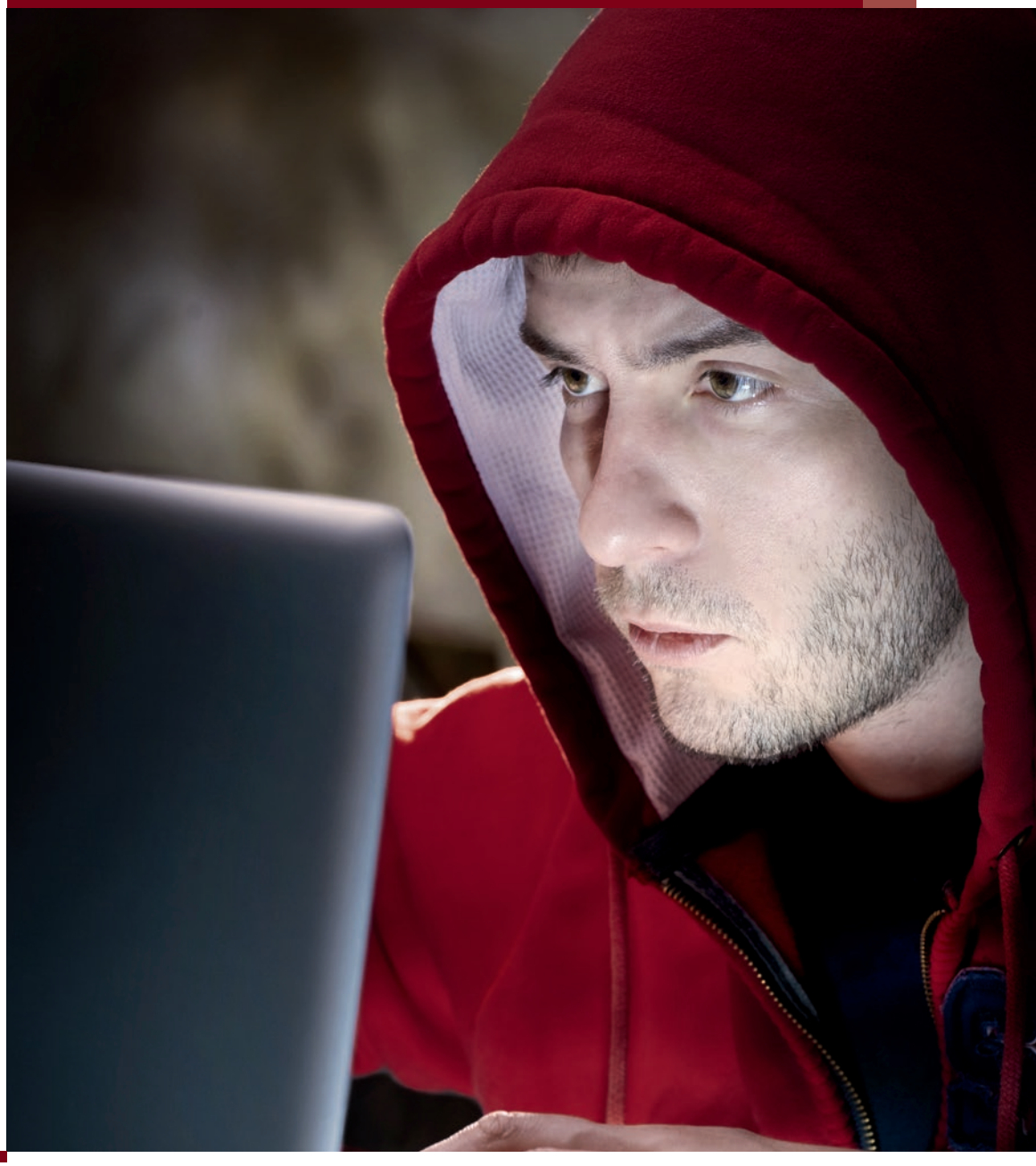
www.pwc.de

Ist Ihr Institut vor Cyber-Angriffen sicher?

Mit der zunehmenden Digitalisierung von Finanzdienstleistungen steigt die Gefahr von Cyber-Angriffen. Wir unterstützen Sie dabei, die Sicherheit Ihrer digitalen Zukunft zu gewährleisten und Ihre Daten vor den Gefahren des Cyber-Raums zu schützen.



pwc

Cyber-Security – unabdingbar für den geschäftlichen Erfolg in der digitalen Zukunft

Der Hintergrund

Durch die kontinuierliche Digitalisierung der Finanzindustrie verändern sich die Anforderungen an die Informationssicherheit stetig. Insbesondere aufgrund der steigenden Abhängigkeit von der IT und den unternehmensübergreifenden digitalen Prozessen erhöhen sich die Angriffsmöglichkeiten aus dem Cyber-Raum. Sie erfordern eine Betrachtung des gesamten digitalen Ökosystems von Banken, Versicherungen und anderen Finanzdienstleistern.

+24 % Die Kosten von Security Incidents bei Finanzdienstleistern sind 2014 im Vergleich zum Vorjahr um 24 Prozent gestiegen.

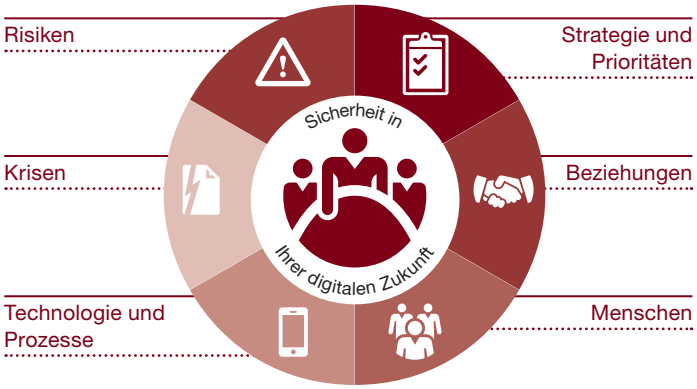
+141 % Die Anzahl der Finanzdienstleister mit Schadensfällen zwischen 10 und 19,9 Millionen Dollar ist um 141 Prozent gestiegen.

Quelle: PwC Global State of Information Security® Survey 2015

Die Herausforderung

Cyber-Risiken müssen erkannt und mit einem ganzheitlichen Blick auf die komplexe Thematik adressiert werden. Neben dem Schutz Ihrer sensiblen Daten vor Angriffen aus dem Cyber-Raum erfordert dies die Berücksichtigung und Umsetzung der stetig steigenden regulatorischen Anforderungen in diesem Bereich.

Die folgenden sechs Dimensionen sind für den Schutz vor Cyber-Angriffen im digitalen Zeitalter von besonderer Bedeutung:



Gleichzeitig werden Cyber-Angriffe immer professioneller sowie zielgerichteter. Sie können bei Erfolg neben einem immensen Reputationsverlust zu direkten finanziellen Schäden in Millionenhöhe führen.

Während Cyber-Angriffe in der Vergangenheit mit einfachen technischen Mitteln oft durch Einzeltäter verursacht wurden, so umfasst die Gruppe der heutigen Angreifer unter anderem Staaten, organisierte Kriminalität und Cyber-Terroristen sowie Insider. Heutige Angreifer verwenden zumeist komplexe, langfristig angelegte und individualisierte Angriffsmethoden, die nicht mehr alleine mit technischem Perimeterschutz abgewehrt werden können. Aufgrund dieser Entwicklung stellt sich inzwischen nicht mehr die Frage, ob, sondern wann ein Angriff stattfindet. Damit werden die Fähigkeiten zum Erkennen von Angriffen und die adäquate Reaktion auf sie wichtiger. Bestehende Sicherheitskonzepte adressieren Cyber-Risiken oftmals nicht oder nur unzureichend.

Diese Entwicklung erfordert eine intensivere Auseinandersetzung mit dem Thema Cyber-Security zur Aufrechterhaltung des Geschäftsbetriebs und dem Schutz von Daten. Daher ist es zwingend erforderlich, die schützenswerten Daten und IT-Systeme zu identifizieren und besonders zu verteidigen. Cyber-Security stellt damit kein reines IT-Thema dar, sondern ist inzwischen eine geschäftliche Notwendigkeit in der Verantwortung des Topmanagements.

Erkennen und Bewerten Ihrer Cyber-Risiken
Die Chancen der Digitalisierung können nicht ohne Kenntnis der damit einhergehenden Cyber-Risiken ergriffen werden. Der Schlüssel zum Erfolg besteht in der Erkennung, Analyse und Bewertung von Cyber-Risiken.

Cyber-Strategie und Prioritäten
Eine Cyber-Security-Strategie sowie die Priorisierung von Schutzmaßnahmen bilden die Leitplanken für den bewussten Umgang mit der Digitalisierung. Sie stellen die Basis dar für den langfristigen Erfolg der Maßnahmen zur Steuerung der Cyber-Risiken.

Sicherheit der Geschäftsbeziehungen
Die Risiken Ihrer Geschäftspartner und Kunden sind auch Ihre Risiken. Gefahren und Risiken durch das wachsende digitale Ökosystem und die engere Verknüpfung und Automatisierung von IT-Systemen und Prozessen über die Unternehmensgrenze hinweg sind stets zu berücksichtigen und zu steuern.

Der Mensch als Risikofaktor
Cyber-Angreifer machen sich zunehmend den Menschen als Sicherheitslücke mittels „Social Engineering“ zunutze. Der Aufbau und die Pflege einer Sicherheitskultur sind mehr denn je nötig, da Ihre Mitarbeiter und Mitarbeiterinnen täglich mit sicherheitsrelevanten Situationen und Entscheidungen konfrontiert sind.

Sicherheit der Technologie und Prozesse
Technologie stützt Ihre Geschäftsprozesse. Da beides einem fortlaufenden Wandel unterliegt, müssen sowohl Ihre neuen IT-Systeme als auch Ihre Altsysteme ausreichend gegen Cyber-Gefahren geschützt werden.

Krisen sicher bewältigen
Cyber-Angriffe gehören zum Alltag. Ein robustes Cyber-Security-Programm umfasst Fähigkeiten zur Erkennung und Analyse von Angriffen sowie zur unverzüglichen Umsetzung von Reaktionsmaßnahmen. So lassen sich die Auswirkungen von Cyber-Angriffen auf Ihren Geschäftsbetrieb begrenzen.

Die Lösung

PwC hat unter Berücksichtigung des NIST CSF (siehe unten) – das unter anderem von der Europäischen Zentralbank als Best Practice Framework genutzt wurde – ein Vorgehensmodell zur Einführung eines wirksamen Cyber-Security-Programms entwickelt. Auf Basis dieses Vorgehensmodells und unserer umfassenden Branchenkenntnisse in der Finanzindustrie begleiten wir Sie

- von der Risikoanalyse im Cyber-Raum
- über die Cyber-Strategie
- bis hin zur Umsetzung von Maßnahmen zum Schutz vor Cyber-Angriffen
- sowie bei ausgewählten Schwerpunktthemen.

Dabei behalten wir stets Ihre individuellen Anforderungen im Fokus, um die für Sie beste Lösung umzusetzen.

NIST Cyber-Security Framework
Das National Institute of Standards and Technology (NIST) hat im Jahr 2014 ein Cyber-Security Framework (CSF) veröffentlicht, welches die sechs beschriebenen Sicherheitsdimensionen umfasst und in fünf Handlungsfeldern Maßnahmen zum Schutz vor Cyber-Risiken vorschlägt:

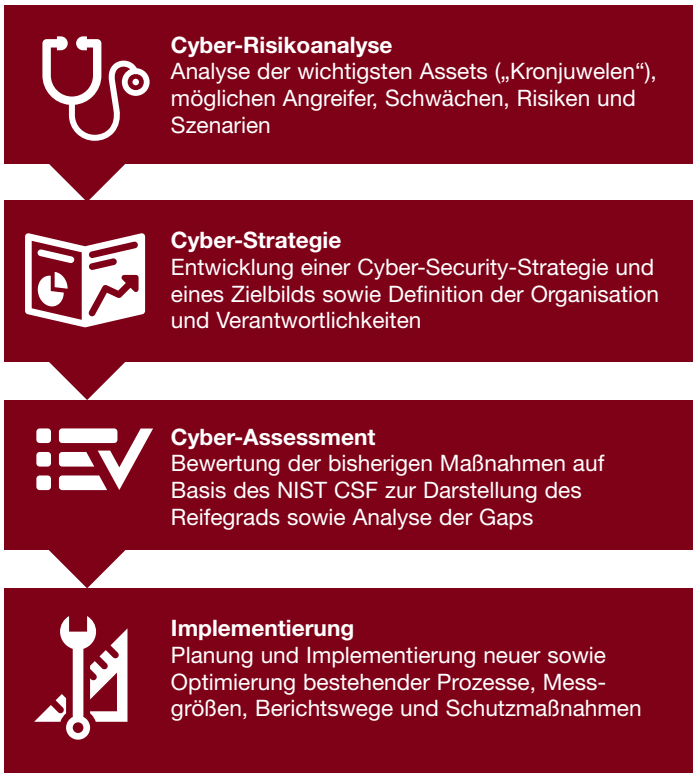
Identify
Verständnis des Managements von Cyber-Risiken und deren Auswirkungen auf IT-Systeme, Daten und Prozesse

Protect
Kontrollen und Schutzmaßnahmen zum Schutz des Unternehmens vor Cyber-Gefahren

Detect
Kontinuierliche Überwachung der IT und Erkennung von Cyber-Angriffen in Echtzeit

Respond
Fähigkeiten zur Analyse und Mitigierung laufender Angriffe sowie zur Begrenzung der Ausweitung und Auswirkungen

Recover
Vorkehrungen und Prozesse zur Aufrechterhaltung und Wiederherstellung des Geschäftsbetriebs



So können wir Sie unterstützen

Cyber-Risikoanalyse
Wir bestimmen gemeinsam mit Ihnen Ihre wichtigsten Assets und unterstützen Sie bei der Analyse Ihrer potenziellen Angreifer aus dem Cyber-Raum. Dies bildet die Grundlage für unsere gemeinsame Bewertung der Cyber-Risiken in Ihrem digitalen Ökosystem.

Cyber-Strategie
Wir helfen Ihnen, eine nachhaltige und langfristige Vision und Roadmap für Ihre Cyber-Security-Organisation zu entwickeln. Dabei berücksichtigen wir die für Ihr Institut relevanten Cyber-Risiken und Angriffspunkte.

Cyber-Assessment
Im Rahmen eines umfassenden Assessments bestimmen wir den aktuellen Reifegrad Ihrer Cyber-Security-Organisation und helfen Ihnen, Handlungsbedarfe zu identifizieren und Investitionen sinnvoll zu priorisieren.

Implementierung
Wir liefern Ihnen spezialisierte Cyber-Security-Services, wie zum Beispiel den PwC Secure Development Lifecycle, die PwC Identity and Access Management Toolbox oder das PwC Penetration Testing Framework. Mithilfe dieser etablierten Tools und Vorgehensweisen unterstützen wir Sie gezielt dort, wo Unterstützung durch unabhängige Experten nötig ist – und helfen Ihnen, Maßnahmen effizient und effektiv zu implementieren und optimieren.

Ihre Ansprechpartner

WP StB Marc Billeb
CISA
Tel.: +49 69 9585-2723
E-Mail: marc.billeb@de.pwc.com

Karsten Wilop
CISA, CGEIT, CRISC
Tel.: +49 211 981-1931
E-Mail: karsten.wilop@de.pwc.com

Achim Schäfer
CISA
Tel.: +49 69 9585-1022
E-Mail: achim.schaefer@de.pwc.com

Dr. Jens Vykoukal
CISA
Tel.: +49 69 9585-6992
E-Mail: jens.vykoukal@de.pwc.com

Unsere Expertise

PwC verfügt weltweit über mehr als 1.600 IT- und Cyber-Security-Experten, darunter mehr als 100 in Deutschland auf Financial Services spezialisierte Mitarbeiter. Unsere Experten haben langjährige Erfahrung in der Beratung und Prüfung von Cyber-Security-Organisationen sowie zu relevanten Schwerpunktthemen (zum Beispiel Informationssicherheitsmanagement, Identity and Access Management, SIEM oder Systemadministration). Mit unserer vielfach bewährten und herstellerunabhängigen Methodik sowie umfassenden Erfahrungen im Rahmen von Beratungsprojekten decken wir alle relevanten Themen im Bereich „Cyber-Security“ vollständig ab.

Zudem erfüllt unser risikoorientiertes Vorgehen durch die Berücksichtigung regulatorischer und gesetzlicher Vorgaben (unter anderem MaRisk, KWG und BDSG) sowie gängiger Standards (unter anderem ISO 2700x, BSI-Grundschutz, COBIT und ITIL) alle Compliance-Anforderungen in der Finanzindustrie. Sie profitieren dabei von unserem risikoorientierten und individuellen Ansatz, mit dem Sie ein wirksames und Compliance-konformes Cyber-Security-Programm umsetzen können. Zusätzlich realisieren Sie Einsparpotenziale bei anderen Prozessen sowie ein erhöhtes Maß an tatsächlicher Sicherheit.

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen 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 Expertennetzwerks in 157 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. 9.400 engagierte Menschen an 29 Standorten. 1,55 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.