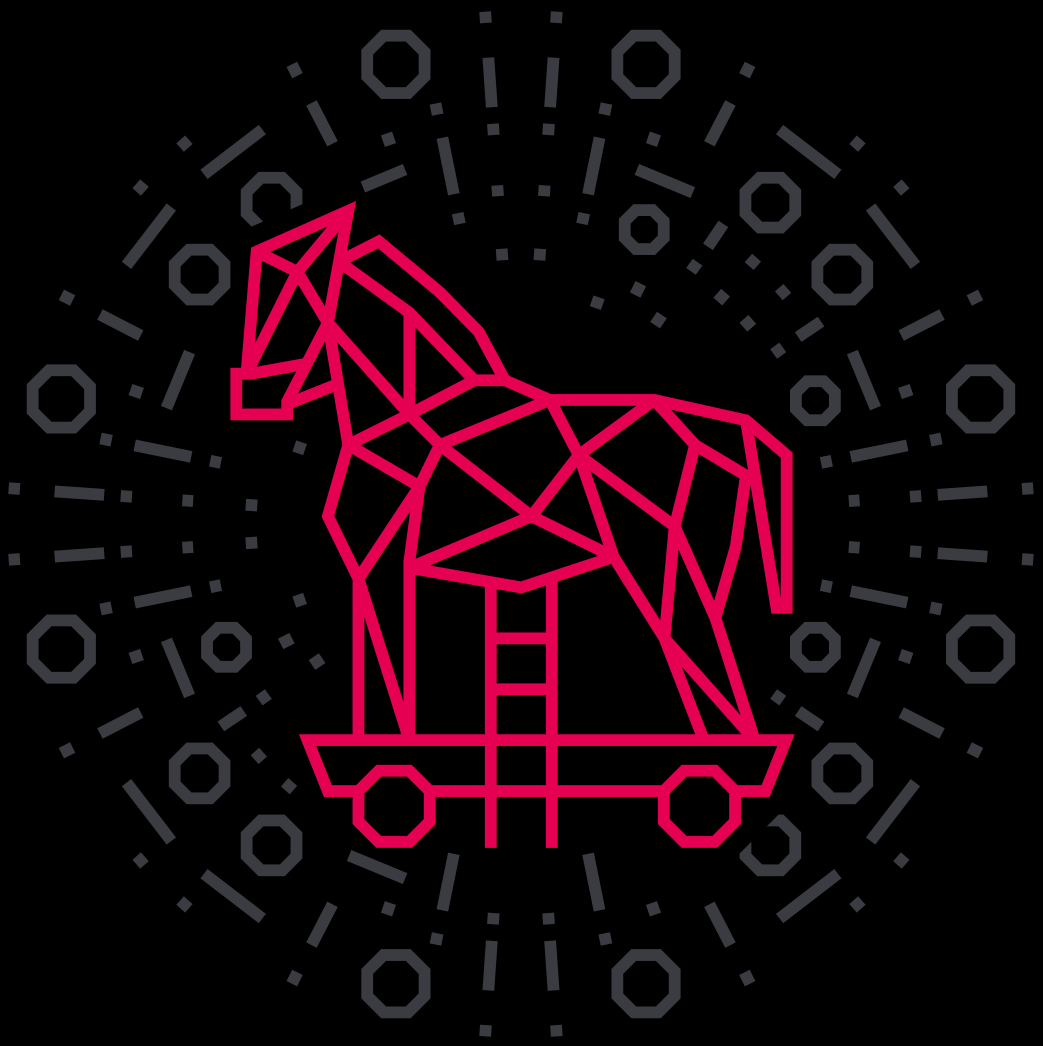
Deloitte.



Red Team

Unser Konzept zur Steigerung organisatorischer Resilienz

Einleitung 03
Unser Selbstverständnis 04
Die Entwicklung des Red Teamings 06
Red Teaming 08
Intel Service 10
Red Team Tests 12
War Games 14
Resilience Training 16
Threat Intelligence-based
Ethical Red Teaming 18
Unser Team 20
Kontakt 22

Einleitung

Das Red Team hat die Mission, die Resilienz von Organisationen gegen feindliche Angriffe nachhaltig zu stärken. Dazu agieren wir aus der Perspektive des Angreifers, um digitale, physische und soziale Schwachstellen aufzudecken und die Reaktionsfähigkeit von Führungskräften und Mitarbeitern unter realen Bedingungen zu testen. Daraus wird ein effektives, maßgeschneidertes Sicherheitstraining für Sie entwickelt und von unseren erfahrenen Experten durchgeführt. Mit unserem Red Team Service können Sie Bedrohungen frühzeitig erkennen, Angriffen vorbeugen und adäquat reagieren, um Vermögenswerte zu schützen und Schäden zu minimieren.

Unser Selbstverständnis

Knut Schönfelder ist Senior Manager bei Deloitte und leitet das Red Team.

Herr Schönfelder, wie verstehen Sie den Begriff „Red Teaming“?
Als das systematische Anwenden von Analysetechniken aus der Sicht eines Angreifers. Ein Red Team hilft so, Unternehmen ihre Annahmen und Pläne kritisch zu prüfen und Schwachstellen zu identifizieren.

Woher kommt das Konzept des Red Teamings?
Red Teaming ist eine Methode, die im Militär des 19. Jahrhunderts entstanden ist. Es wurde erkannt, dass es Umstände gibt, die bei der ursprünglichen Planung nicht berücksichtigt wurden, die das Gelingen des Plans jedoch gefährden können. Die Konfrontation des gedachten Vorgehens mit möglichen Unwägbarkeiten hat sich als Methode zur kritischen Überprüfung durchgesetzt. Heute werden im Militär Schwachstellen in den bestehenden und geplanten Verfahren regelmäßig von Red Teams aufgedeckt.

Wir als Red Team sind an der sinnvollen Übertragung dieses bewährten Prinzips auf die uns umgebende, globalisierte Handelswelt interessiert. Für heutige Unternehmen und Konzerne bietet ein geschultes Red Team eine naheliegende Möglichkeit, sich zu einer resilienten, also widerstands- und anpassungsfähigen, Organisation zu entwickeln.

Wenn man den Begriff „Red Teaming“ im Internet sucht, findet man ganz verschiedene Angebote und Beschreibungen. Was macht das Angebot von Deloitte zu etwas Besonderem?
Viele dieser Angebote umfassen nur Teilaspekte unserer Dienstleistung. Für uns ist Red Teaming deutlich mehr als ein Penetrationstest, bei dem sich Hacker einen neuen Weg in ein Firmennetzwerk suchen. Wir wollen auch die Auswirkungen von Angriffen abschätzen, vorab eine Risikoanalyse erstellen und mit unseren Maßnahmen systematisch die organisatorische Resilienz steigern.

Deloitte bietet demnach ein umfangreiches Red Teaming?
Unser Angebot versteht sich als kontinuierlicher Service, der über die Cyber-Welt hinausgeht. Zudem vereinen wir vier für uns zentrale Elemente: Intel Service, War Games, Red Team Tests und Resilience Training. Dabei liefert unser Intel Service Analysen, stellt Szenarien bereit und bringt somit den Stein ins Rollen. Mit so genannten War Games und Red Team Tests fordern wir unsere Kunden regelmäßig auf

„Red Teaming ist das systematische Anwenden von Analysetechniken aus der Sicht eines Angreifers.“

unterschiedlichsten Ebenen heraus. War Games trainieren die internen Entscheidungsprozesse in besonderen Situationen, Red Team Tests untersuchen Organisationen auf Schwachstellen und verifizieren diese. Unsere Erkenntnisse fassen wir kontinuierlich in verschiedenen Reports zusammen und lassen erkannte Defizite in ein Resilience Training einfließen, welches wir gemeinsam mit unseren Auftraggebern durchführen. Dabei beschäftigen wir uns zudem mit Annahmen und Einschätzungen, die in den von uns betreuten Unternehmen vorherrschen. Diese stellen sich oftmals als unerwiesen oder ungewiss heraus (englisch „Bias“) und können so, möglicherweise, ein falsches Gefühl von Sicherheit suggerieren.

Wie setzt sich das Team zusammen?
Ein weiteres Unterscheidungsmerkmal sehe ich in der, wie ich finde, einzigartigen Zusammensetzung des Deloitte Red Teams. Es vereint Cyberexperten, Politikwissenschaftler, Wirtschaftswissenschaftler, Ingenieure, Experten für Social Media Analysen und Intelligence-Experten, mit einer Mischung aus zivilen und militärischen Hintergründen. Mit dieser Kombination schaffen wir es, beinahe jeden kreativen Blickwinkel in unserem Vorgehen zu berücksichtigen.

Sie sagen selbst, dass Red Teaming an sich nichts Neues darstellt. Warum ist es heute wieder wichtig?
Es ist noch immer wichtig – sogar wichtiger denn je! Wir alle leben in der wohl schnelllebigsten und komplexesten Welt der Geschichte. Ständig wechselnde Anforderungen prägen unser Leben. In dieser Welt leben auch unsere Staaten und Unternehmen. Als Konsequenz daraus geht die Entwicklung von auch zukünftig sicheren Systemen und Organisationsformen weg von starrer und als belastend empfundener Sicherheit, hin zu flexibler Resilienz. Anstatt nur immer größere Mauern aufzubauen, helfen wir, mit Angriffen aktiv und souverän umzugehen und sie so zu entkräften. Hierzu gibt es auf europäischer Ebene bereits gute Ansätze, vor allem für das Finanzwesen, auf welche wir unter anderem mit unserem System aufbauen. Insgesamt bringt ein gutes Red Teaming die Resilienz einer Organisation entscheidend und vor allem lebhaft voran.

„Unser Angebot versteht sich als kontinuierlicher Service, der über die Cyber-Welt hinausgeht.“

Das klingt nach einer Mammutaufgabe …
… der wir uns, mit dem von unserem Team entwickelten System, selbstbewusst stellen. Wir sind dabei nicht allein. Neben unserer eigenen Arbeitskraft als Red Team, erhalten wir gerade in dem Bereich unseres Intel Service, mit dem wir unseren Kunden alle notwendigen Analysen bereitstellen, wertvolle Unterstützung aus vielen Bereichen von Deloitte. So kooperieren wir beispielsweise sehr erfolgreich mit dem von Deloitte entwickelten Künstliche-Intelligenz-Tool Deloitte Gnosis, welches es uns erlaubt Zukunftsszenarien zu erstellen und damit Prognosen für bevorstehende Bedrohungen und Entwicklungen abzugeben.

Natürlich profitieren wir als ein Team von Deloitte auch von dem umfassenden Netzwerk und Erfahrungsschatz anderer Kollegen aus den Bereichen Wirtschaftsprüfung, Beratung, Finance und vielen mehr. Das Gesamtprodukt aller Erfahrungen und Erkenntnisse geben wir gern an die Kunden unseres Red Team Service weiter.

„Tell me things others don't, and make senior officials feel uncomfortable."

George Tenet
ehemaliger Leiter der CIA

Die Entwicklung des Red Teamings

Red Teaming ist eine Methode, die im Militär des 19. Jahrhunderts entstanden ist, ursprünglich in der Ausbildung preußischer Offiziere. Man wollte damit die als Friktionen bezeichneten Unwägbarkeiten in militärischen Auseinandersetzungen besser beherrschen. Wetter, das Gelände, fehlende oder falsche Informationen, Probleme in der Versorgung, Verlagerung und Wirkung der eingesetzten Truppen, all dies hatte unkalkulierbare Auswirkungen auf den Erfolg eines ursprünglichen Plans.

Historisch bedeutend ist das „taktische Kriegsspiel" des Barons von Reißwitz. Der ursprüngliche Apparat, im Berliner Schloss Charlottenburg zu besichtigen, war ein Brettspiel bestehend aus Terrainsteinen und Spielmarken mit dem, basierend auf einem detaillierten Regelwerk, Schlachtverläufe simuliert wurden. Zwei Parteien mussten, Zug um Zug, ihre Operationspläne durchsetzen. Jeder Zug hatte in exakt zwei Minuten zu erfolgen, angelehnt an die Dauer eines Artilleriefeuers. Neben der Entscheidung zum Einsatz der eigenen Truppen wurde der Verlauf des Gefechts durch Würfelspiele, stellvertretend für die unkalkulierbaren Friktionen, bestimmt.

Diese ursprüngliche Methodik des Kriegsspiels wird heute zumeist als „War Game" bezeichnet und ist zum integralen Bestandteil des Planungsprozesses geworden.

Ausgehend von der zeitlich begrenzten Analyse eines vorher ausgewählten Szenarios im Rahmen eines War Games, ist die Praxis des Red Teamings entstanden. Organisationen – neben dem Militär heute auch zivile Unternehmen – prüfen durch eigens dafür aufgestellte Red Teams ihre Annahmen und Pläne kritisch. Sie identifizieren Schwachstellen und erlangen ein besseres Verständnis ihres operativen Umfeldes, insbesondere im Cyber-Umfeld.

Ein aktuelles Beispiel ist der US-Auslandsgeheimdienst CIA. Am Tag nach den Anschlägen des 11. September machte George Tenet, damals Direktor der CIA, eine ebenso kurze, wie ungewöhnliche Vorgabe: Er ordnete die Aufstellung einer CIA Red Cell genannten Einheit an. Deren Auftrag: Das liefern von Informationen, die sonst niemand liefert und die Entscheidungsträgern Sorgen bereiten. Warum das ungewöhnlich ist? Weil Tenet an sich eine Behörde leitete, deren Hauptaufgabe ohnehin der Gewinn und die Auswertung von Informationen zur nationalen Sicherheit ist. Nach den verheerenden Anschlägen wollte er jetzt ein Team, das die bisherige konventionelle Denkweise ebenso radikal wie systematisch in Frage stellt und so die Gefahr weiterer überraschender Terror-Angriffe minimieren sollte.

Red Teaming

Wir sind überzeugt: Egal wie gut sich eine Organisation gegen Angriffe schützt, es wird immer eine neue Schwachstelle geben. Sicherheit ist immer nur ein temporärer Zustand – das Risiko eines erfolgreichen Angriffs bleibt. Neben präventiven Schutzmaßnahmen ist organisatorische Resilienz, d.h. die Fähigkeit zur Aufrechterhaltung bzw. Wiederherstellung von Geschäftsprozessen nach einer Störung, ein wichtiges Element der IT- und Unternehmenssicherheit.

Organisatorische Resilienz bedingt die Fähigkeit Bedrohungen zu antizipieren, sich auf mögliche Angriffe vorzubereiten, die schädlichen Auswirkungen von Angriffen zu minimieren und zu tolerieren, um schließlich die Geschäftstätigkeiten möglichst schnell wieder aufnehmen zu können und ggf. die eigenen Sicherheitsmaßnahmen anzupassen. Um resilient zu sein, muss eine Organisation:

- Informationen zu bestehenden Risiken aus geeigneten Quellen beschaffen
- die richtigen Schlüsse aus diesen Informationen ziehen
- sich dabei des Einflusses von kognitiven und sozialen Aspekten auf die Entscheidungsfindung bewusst sein und
- angemessene technische und organisatorische Sicherheitsmaßnahmen einleiten und ihre dauerhafte Wirksamkeit sicherstellen

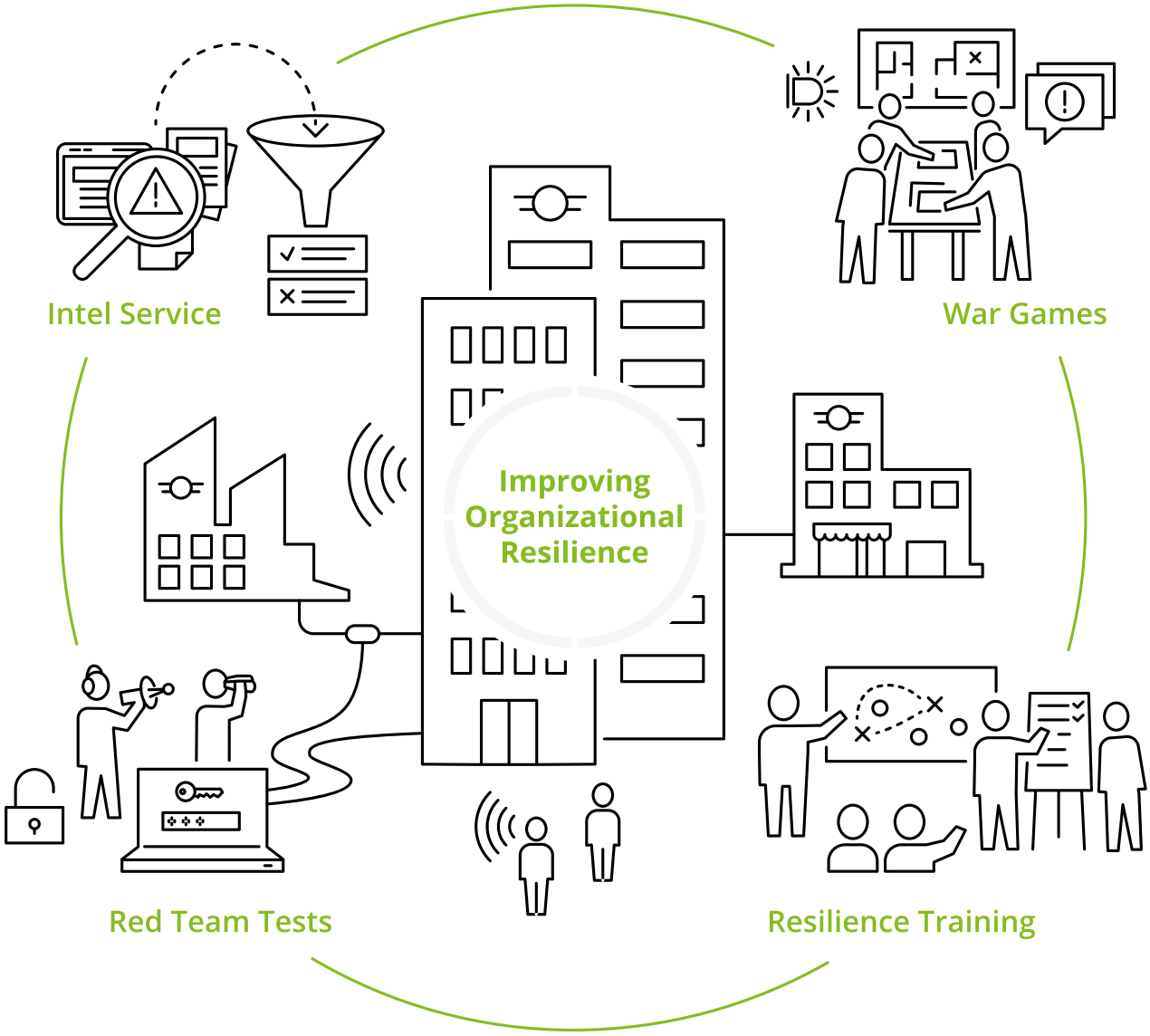
Mit unserem kontinuierlichen Red Teaming Service wollen wir Unternehmen in diesem Prozess unterstützen. Ausgehend von einer gemeinsamen Bewertung des Status quo der organisatorischen Resilienz gewährleisten wir durch eine individuelle Kombination unserer vier Service-Elemente:

- kontinuierliche Bereitstellung von Informationen zu Risiken und relevanten Bedrohungen
- Durchführung regelmäßiger Tests zur Aufdeckung und Validierung von Schwachstellen
- Simulationen von realitätsnahen Angriffszenarien, um mögliche schädliche Auswirkungen zu bewerten
- Entwicklung und Begleitung eines auf den spezifischen Bedarf des Unternehmens ausgerichteten Trainings- und Ausbildungsprogramms

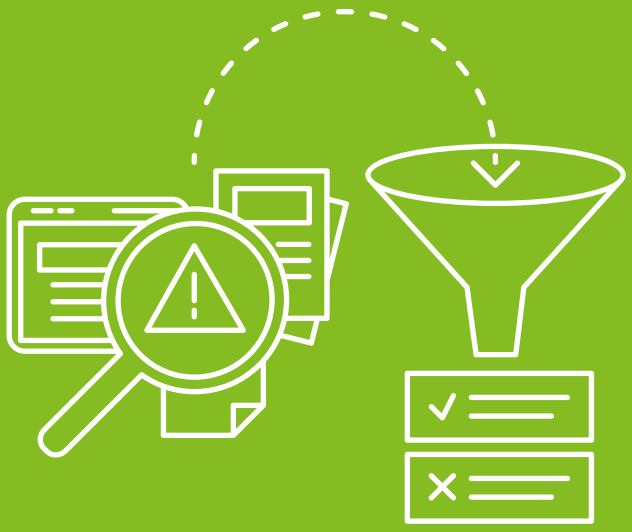
Unser bewährtes Resilience Framework, eine unterstützte Selbsteinschätzung, dient dabei als Referenz, um den Stand der organisatorischen Resilienz festzustellen, zu überwachen und den Effekt unserer Maßnahmen zu bewerten.

„Security is a process not a product!“

Bruce Schneier

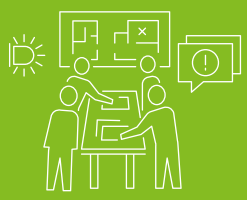


Die vier Elemente des Red Teamings



Intel Service

Red Team Tests



War Games

Resilience Training

Intel Service

Zur Verbesserung der Resilienz, der universellen Widerstands- und Anpassungsfähigkeit, ist ein gutes Verständnis von Risiken und Bedrohungen unerlässlich.

Der englische Begriff „Intelligence“ oder auch „Intel“ hat seinen Ursprung im Militär und den Nachrichtendiensten (engl.: „Intelligence Services“) und bezeichnet die Beschaffung, Sammlung, Auswertung und Bewertung von Informationen zu einem bestimmten Zweck. Die genaue Kenntnis der komplexen und schnelllebigen Entwicklungen in diesem Bereich bildet die Basis allen, auf Resilienz fokussierten, Handelns.

Unser Intel Service stellt unseren Kunden nutzbare Bewertungen zur Verfügung, die einen 360-Grad-Blick auf die bestehende, individuelle Bedrohungslandschaft erlauben. Darüber hinaus erarbeiten wir mit den von uns betreuten Unternehmen, auf diesen Erkenntnissen aufbauende Szenarien, mittels derer die Resilienz unserer Kunden gesteigert und langfristig erhalten bleiben kann.

Für unser Angebot sind zwei Bereiche wesentlich: Erstens sind die Qualität und Diversität der zugrundeliegenden Informationen von zentraler Bedeutung. Die kontinuierliche, professionelle Auswertung und Bewertung dieser Informationen ist der zweite entscheidende Baustein unserer Dienstleistung.

Unsere Informationsbeschaffung ist vor diesem Hintergrund äußerst breit und vielfältig angelegt. Open Source Intelligence (OSINT) ist ein zentrales Element dieses Prozesses. Hierbei wird vornehmlich das Internet nach geeigneten Informationen durchsucht. Dies schließt bei uns neben erweiterten, von Analysten gesteuerten Suchläufen mittels Suchmaschinen, explizit das Deep- und Dark-Web ein. Softwares und Tools, wie das Deloitte Gnosis, erlauben uns mittels künstlicher Intelligenz (KI) zielgerichtet, relevante Informationen aus abertausenden Primärquellen zu erhalten und einzuordnen.

Der Intel Service bindet unsere Kunden zu jeder Zeit ein. Neben einer von uns entwickelten, standardisierten Selbsteinschätzung, die als wichtiger Indikator dient, planen und gestalten wir in Workshops gemeinsam mit den Nutzern unseres Angebots mögliche Angriffsszenarien. Die Entwicklung dieser Szenarien basiert auf statistischen Annahmen, die mit den Zielen unserer Kunden in Verbindung gesetzt werden und es uns erlauben, Prognosen für eine zukünftige Bedrohungslandschaft abzugeben.

Red Team Tests

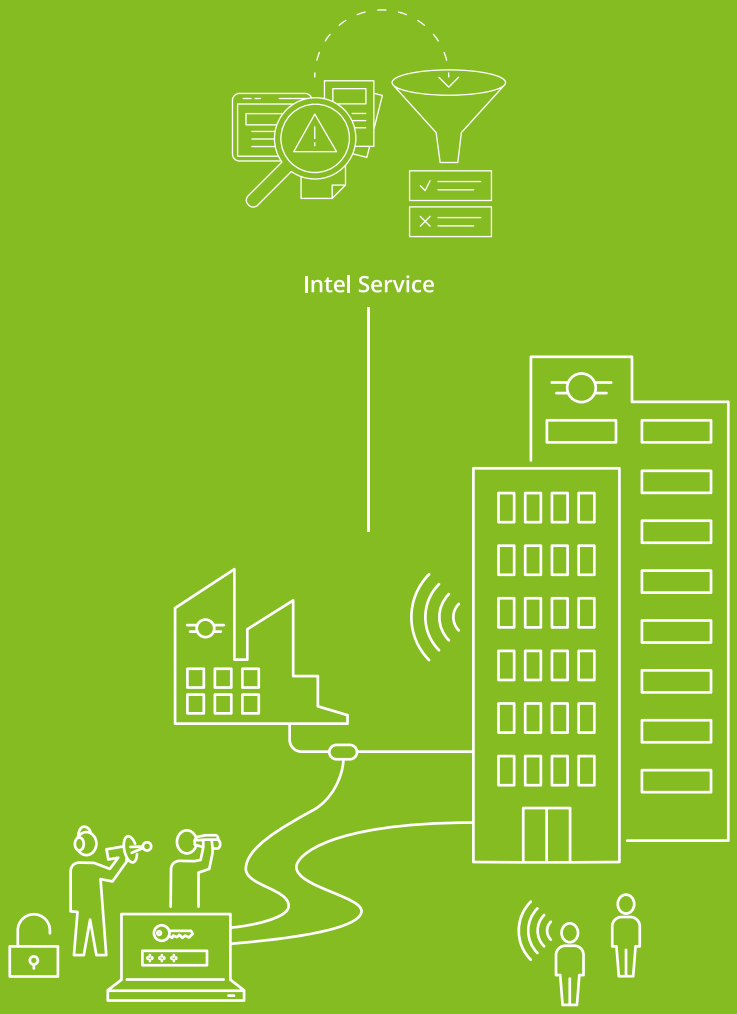
In unseren Red Team Tests simulieren wir einen realistischen Angriff auf ein Unternehmen. Wir identifizieren Schwachstellen und demonstrieren wie diese ausgenutzt werden können, um kritische Prozesse zu stören, Systeme anzugreifen oder vertrauliche Informationen zu entwenden. Der Zweck eines Red Team Test ist es, die Resilienz einer Organisation zu bewerten.

Unsere Tests basieren auf konkreten Angriffsszenarien und einer vorherigen Analyse der Bedrohungslage. Sie beinhalten Aussagen zu möglichen Typen von Angreifer mit spezifischer Absichten, Expertise und Fähigkeiten. Jedes Szenario hat ein konkretes Angriffsziel. Es erfolgt auch eine Abschätzung, welcher Schaden bei einem erfolgreichen Angriff erzeugt werden würde.

Das Red Team demonstriert im Rahmen des Tests, wie Schwachstellen und Angriffswege so ausgenutzt werden könnten, dass die Organisation geschädigt wird, z. B. durch die simulierte Störung kritischer Prozesse oder den Diebstahl vertraulicher Daten. Wenn das Red Team derartige Angriffsszenarien entwickelt, bewerten wir physische Sicherheitsmaßnahmen, die Sicherheit des Netzwerkes, von Applikationen und Systemen aber auch die Möglichkeit zur bewussten Manipulation von Mitarbeitern (Social Engineering). Die Angriffsszenarien enthalten physische Angriffselementen, Social Engineering und Hacking-Techniken die so kombiniert werden, dass das Red Team sein Angriffsziel erreichen kann. Denkbare Elemente eines Red Team Tests sind:

- Versuche zur bewussten Beeinflussung von Mitarbeitern, um vertrauliche Informationen zu gewinnen oder um sie zu einer unbewussten Unterstützung des Angriffsplans zu bewegen
- Aufklärung des Unternehmensgeländes und der Sicherheitsmaßnahen, um Schwachstellen zu identifizieren und unbemerkt in abgesperrte Bereiche einzudringen
- Nutzung angemessener Werkzeuge und Techniken, um in das Netzwerk einzudringen, Applikationen zu manipulieren und so systematisch zu der Zielressource vorzudringen

Unsere Tests ermöglichen es abzuschätzen, ob angemessene Sicherheitskontrollen implementiert und eingesetzt werden. Ziel ist eine realistische Bewertung der organisatorischen Resilienz. Im Vorfeld und während des Red Team Tests stimmen wir uns eng mit unseren Kunden ab, um Einschränkungen oder Vorgaben zu definieren und zu überwachen. Der Test Report beinhaltet eine detaillierte Beschreibung der gewählten Vorgehensweise sowie eine Darstellung der Testergebnisse und -erkenntnisse. Ebenfalls erfolgt eine Einordung ihrer Bedeutung für die Resilienz des Unternehmens. Ergänzend geben wir erste Empfehlungen für eine Optimierung technischer Kontrollmaßnahmen, Prozesse, Regelwerke, Richtlinien und Ressourcen.

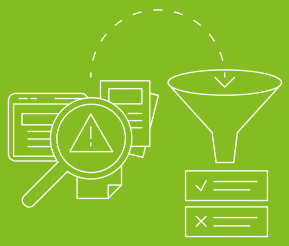


Intel Service

Red Team Tests

War Games

Resilience Training



Intel Service

Red Team Tests

War Games

Resilience Training

War Games

War Games sind szenariobasierte Simulationen, mittels derer die Reaktionsfähigkeit einer Organisation herausgefordert und überprüft wird. Die Mitglieder von Krisenstäben sind die zentralen Akteure dieser Übungen.

Unternehmenskrisen gestalten sich facettenreich und können spontan und unvermutet jede Organisation treffen. Diverse Krisen der Vergangenheit haben gezeigt, dass ein rasches, zielgerichtetes Handeln das Ausmaß einer Krise deutlich einzudämmen vermag. Ein eingespielter, zügig und sicher handelnder Krisenstab ist ein bedeutender Eckpfeiler einer resilienten Organisation. Zum Aufbau und Erhalt einer angemessenen Reaktionsfähigkeit ist, neben einer soliden Dokumentation der notwendigen Abläufe und Verfahren, regelmäßiges Training der Handelnden unerlässlich.

Im Zuge der von uns durchgeführten War Games werden Krisenstäbe in sicherem Umfeld auf den Ernstfall vorbereitet und trainiert. Umfang und Szenario der Übungen werden im Vorfeld eigens abgestimmt und an den Bedarf und die Fähigkeiten unseres Kunden angepasst.

Die Auswahl eines passenden Szenarios wird dabei maßgeblich durch die mittels unseres Intel Service ermittelten Wahrscheinlichkeiten geprägt. Unsere Kunden haben damit die Möglichkeit, ihre internen Kompetenzen unter Anleitung zu verbessern und zeitgleich an einem für die Organisation essentiellen Szenario zu üben und somit die Organisation direkt auf eine mögliche Krise vorzubereiten.

Da Unternehmenskrisen wenig vorher sehbar und in ihren Ausprägungen in hohem Maß mannigfaltig sind, zielen unsere War Games nicht auf das Vorproben bestimmter Fälle, sondern auf individuell anpassbare Stabsarbeit ab. Sicher einstudierte Handlungsmuster bieten in Stresssituationen den notwendigen Rückhalt.

Diese Handlungssicherheit wird durch unser Team während der War Games dauerhaft herausgefordert. Die Reaktionen des Krisenstabes rufen dabei eine erneute Gegenreaktion unseres Red Teams hervor, sodass sich ein spielerischer Wettkampf zwischen zwei Teams entwickelt.

Die Fähigkeit der handelnden Akteure auf jedwede Situation zu reagieren, ist unmittelbares Indiz für die Resilienz des Unternehmens.

Resilience Training

Mittels unseres Resilience Trainings schließen wir gemeinsam mit unseren Mandanten alle erkannten Schwachstellen und Trainingsdefizite.

Wir sind dauerhafter Sparringpartner unserer Kunden. Das alleinige Erkennen von Handlungsfeldern durch Intel Service, Red Team Testing und War Gaming schafft keine höhere Belastbarkeit.

Fortdauerndes, zielorientiertes Training unter Einbezug aller relevanten Akteure garantiert maximalen Erfolg auf dem Weg zu einer resilienten Organisation.

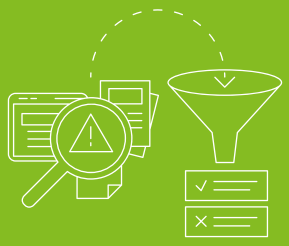
Unser Training fußt auf der Identifikation der zu trainierenden Themenfelder. Diese stimmt unser Team gemeinsam mit Ihnen als Kunden ab und bezieht sich dabei unter anderem auf Ihre Selbsteinschätzung. Darauf aufbauend schließen wir unsere Erkenntnisse aus den Bereichen Intel Service, Red Team Tests und War Games in die Gestaltung des Trainingsprogramms ein. Die genaue Zielgruppe einzelner Trainings wird gemeinsam mit unseren Kunden für jeden Themenbereich festgelegt. So kann das individuelle Trainingsprogramm zielgerichtet notwendige Teilnehmer erreichen und maximalen Mehrwert liefern. Umfang und Art des Trainings werden dabei genau auf die Bedürfnisse unserer Kunden ausgerichtet und fortwährend angepasst.

Unsere erfahrenen Trainer begleiten die Trainingsgruppen über mehrere Stationen. Dabei greifen sie auf ihre Expertise in verschiedenen Fachrichtungen zurück und stellen so ein ganzheitliches Lernkonzept sicher. Die Trainingsmöglichkeiten reichen dabei von Awareness-Schulungen, über Stabstrainings, hin zu konkreten Verbesserungen organisatorischer und struktureller Gegebenheiten.

Ein Beispiel eines solchen Trainings ist das Bias Testing. Hier geht es darum, sich unbewusst vorherrschende Biases, also Denkfehler, bewusst zu machen und konkrete, mentale Mechanismen zum Schutz vor diesen Fehlannahmen bei den Mitarbeitern zu etablieren. Bias Testing und Training hilft dabei, durch menschliche Komponenten entstehende Schwachstellen zu reduzieren oder zu vermeiden und wird durch im Red Teaming ausgearbeitete Handlungsoptionen effektiv gestärkt.

Der Lernerfolg unserer Kunden wird von unserem Team begleitet, Trainingspläne laufend angepasst. Somit können wir individuell auf die Bedürfnisse unserer Kunden eingehen und die Weiterentwicklung einzelner Zielgruppen innerhalb des Unternehmens aktiv steuern. Dies ist ein wichtiger Bestandteil zum Auf- und Ausbau der Resilienz des Unternehmens und trägt maßgeblich zum Abbau aktueller und zur Vermeidung zukünftiger Schwachstellen bei.

Unser Resilience Training vervollständigt somit den Kreislauf der vier Kernelemente unseres Red Teaming Angebots.



Intel Service

Red Team Tests

War Games

Resilience Training

Threat Intelligence-based Ethical Red Teaming

Die rapide wachsenden Sicherheitsherausforderungen sind nicht nur für einzelne Unternehmen ein Kernthema, sondern auch auf nationaler, europäischer und internationaler Ebene ein wichtiger Diskussionspunkt.

Im Mai 2018 hat die Europäische Zentralbank (EZB) das *Framework for Threat Intelligence-based Ethical Red Teaming*, kurz TIBER-EU, verabschiedet. TIBER-EU bietet europäischen und nationalen Institutionen sowie Behörden im Finanzsektor (und darüber hinaus) einen gemeinsamen Rahmen, um durch Red Teaming ihre bestehenden Systeme auf Schwachstellen zu testen und die Resilienz gegen komplexe Cyberangriffe auszubauen. Das TIBER Framework basiert auf systematischen, organisationsspezifischen und Threat Intelligence-basierten Red Team Tests. Durch simulierte Angriffe sollen die kritischen Funktionen und Systeme (d. h. Menschen, Technologie und Prozesse) nachhaltig gestärkt und gesichert werden.

Der TIBER-EU-Prozess besteht aus einer optionalen, einleitenden Phase sowie aus drei obligatorischen Phasen:

Generic Threat Landscape Phase

In der (optionalen) Generic Threat Landscape Phase wird ein Lagebild zu den Risiken und Bedrohungen im nationalen Finanz-Sektor erstellt. Dazu werden die maßgeblichen Akteure und ihre spezifischen Techniken, Taktiken und Vorgehensweisen (TTPs: Techniques, Tactics and Procedures) analysiert. Dies ist die Grundlage für die spätere Entwicklung von Angriffsszenarien. Die Generic Threat Landscape wird regelmäßig aktualisiert, um den Auftritt neuer Akteure und TTPs zu berücksichtigen.

01. Preparation Phase

Diese Phase beinhaltet den formalen Start der TIBER-EU Tests, einschließlich der Aufstellung der Teams die für die Durchführung der Tests verantwortlich sind. Außerdem wird die Zielsetzung der Tests festgelegt, dem Vorstand der Institution vorgelegt und durch die relevanten Aufsichtsbehörden bestätigt. Abschließend werden die Threat Intelligence und Red Team Dienstleister mit der Durchführung der Tests beauftragt.

02. Testing Phase

Die Testing Phase besteht aus der Threat Intelligence Analyse und den Red Team Tests. Der Threat Intelligence Dienstleister erstellt einen Targeted Threat Intelligence Report (TTI) für die jeweilige Institution. Dieser Report umfasst die spezifischen Bedrohungsszenarien für die folgenden Red Team Tests. Das Red Team leitet aus diesen Bedrohungsszenarien konkrete Angriffsszenarien ab und testet in diesem Rahmen kritische Systeme, organisatorische Strukturen und Prozesse.

03. Closure Phase

In der abschließenden Closure Phase werden Folgemaßnahmen vereinbart und die Ergebnisse der Tests angemessen kommuniziert. Das Red Team erstellt einen Report der eine detaillierte Darstellung der Vorgehensweise und Ergebnisse der Tests enthält. Wenn erforderlich, enthält der Report konkrete Empfehlungen zu technologischen Kontrollmaßnahmen, Regularien und Verfahren. Abschließend nimmt die getestete Institution den Report mit allen Testergebnissen formal zur Kenntnis und erstellt – in Zusammenarbeit mit den zuständigen Aufsichtsbehörden – einen Maßnahmenplan.

TIBER-EU-Prozess

Dabei müssen TIBER-EU Tests von unabhängigen, externen Anbietern durchgeführt werden. Dies gilt sowohl für den Bereich Threat Intelligence (TI) als auch den Bereich Red Teaming (RT). Der externe Dienstleister führt dabei in Kooperation mit der Instanz die Tests durch und fertigt die notwendigen Analysen in Form eines Targeted Threat Intelligence Reports und eines Red Team Test Reports an.

Das Red Team bietet mit seinem Ansatz individualisierte Lösungen aus einer Hand. Mit unserer weitreichenden Erfahrung und unseren interdisziplinären Kompetenzen können wir den Gesamtprozess des TIBER-EU Frameworks von Anfang bis Ende abbilden und sowohl Threat Intelligence als auch Red Teaming mit unserem Team abdecken. Die weitgefächerte, tiefgehende Expertise unseres Teams ermöglicht dabei ein konkretes Eingehen auf die Bedürfnisse und Gegebenheiten jedes einzelnen Kunden. Wir bieten eine maßgeschneiderte Lösung mit maximaler Wirkungskraft innerhalb des durch das TIBER-EU Framework abgesteckten Rahmens.

Ein besonderer Ansatzpunkt für unser Team ist hier die Erstellung der „Generic Threat Landscape" im ersten Prozessschritt. Dieser greift die größten Bedrohungen für den Bankensektor auf und liefert die Grundlage für die Entwicklung von Angriffsszenarien für die Red Teaming Tests. Ebenfalls kann diese Bedrohungslandschaft in den Targeted Threat Intelligence Report mit einfließen. Daher kommt ihm eine ausgesprochen große Wichtigkeit zu. Zur Erstellung dieser Generic Threat Landscape nutzt das Red Team eine Kombination aus bewährten Threat Intelligence Techniken und innovativer AI (Künstlicher Intelligenz). Dabei liegt der Schwerpunkt nicht nur auf aktuellen Bedrohungen für den Kunden, sondern auch auf zukünftigen Trends und Entwicklungen. Um den kontinuierlichen Nutzen der Red Teaming Ergebnisse zu gewährleisten und unseren Kunden dauerhaft zur Seite zu stehen, setzt der Red Teaming Ansatz nicht nur bei einmaligen Tests und Reports an, sondern stellt ein dauerhaftes Monitoring in Aussicht. Nur so kann die Resilienz eines Kunden in Hinblick auf das sehr dynamische und hochkomplexe Cyber- und Sicherheitsfeld langfristig und nachhaltig gewährleistet werden. Hierzu arbeitet das Red Team eng mit dem Deloitte Center for the Long View zusammen. Durch Szenarioplanung werden Zukunftstrends erfasst, Strategien getestet und mit Hilfe unseres AI-Tools Deloitte Gnosis langfristig überwacht. So kann die erstellte Generic Threat Landscape nicht nur aktuell gehalten werden, sondern auch konkret auf neue, zukünftige Bedrohungen eingehen. Gemeinsam mit unserem innovativen Red Teaming Ansatz kann der Kunde über das TIBER-EU Framework hinaus optimal und individuell betreut werden.

TIBER-EU – Konkrete Ziele:

- Ausbau der Cyberresilience in den Zielinstanzen und im Finanzsektor allgemein
- Standardisierte und harmonisierte Red Teaming Abläufe innerhalb der EU mit ausreichender Flexibilität zur Anpassung an nationale Gegebenheiten
- Handreichung eines Leitfadens für Behörden zur Etablierung, Implementierung und Management von Red Teaming auf nationalem und europäischen Level
- Unterstützung von grenzübergreifendem Red Teaming für multinationale Instanzen
- Ermöglichung eines Austausches zwischen Behörden durch gemeinsame standardisierte Red Teaming Prozesse und dadurch regulatorische Entlastung einzelner Mitgliedsstaaten
- Erstellung eines gemeinsamen Protokolls zu einer grenzübergreifenden Kollaboration, Ergebnisaustausch und Analyse

Unser Team

Unser Red Team bündelt Expertenwissen aus den verschiedensten Gebieten.

Das interdisziplinäre Team besteht aus Cyberspezialisten, Wirtschaftsexperten, Informatikern, Intelligence Analysten, ehemaligen (Stabs-) Offizieren und Politikwissenschaftlern und deckt damit die zentralen Felder im Bereich Organisational Resilience ab. Somit verkörpert das Red Team, neben dem relevanten Fachwissen, alle wichtigen Eigenschaften, die die vier Kernelemente des Red Teamings definieren: exzellente Analyse- und Recherchefähigkeiten im Bereich Intel Service, weitreichende praktische Strategie- und Taktikerfahrung in militärischen und zivilen Simulationen im War Gaming. Hinzu kommen Kreativität, Voraussicht und ein großer Erfahrungsschatz im Red Team Testing. Konkrete, branchenspezifische Erfahrung in der Erstellung und Durchführung von Entwicklungsplänen runden das Fähigkeitsspektrum in der Disziplin Resilience Training ab.

Unsere Spezialisten bringen ihre individuelle Erfahrung in Threat Intelligence, Open Source Intelligence, Social Media Analysis, Social Engineering, Penetration Testing, Red Team Testing, War Gaming und Trendanalyse in allen Elementen unseres Red Teamings ein. Unterstützt wird unser Team durch die Technologien und Kompetenzen des Deloitte Cyber Intelligence Centers (CIC) in Frankfurt. Dies ermöglicht eine holistische Ansicht auf mögliche Bedrohungsszenarien und Resilienzstrategien.

Das Deloitte Netzwerk
Zur stetigen Optimierung unserer Arbeit greift das Red Team auf das weitreichende internationale Deloitte Netzwerk zurück. Eine Vielzahl von Kooperationen mit Deloitte-eigenen Expertenzentren ermöglicht das Einbringen bahnbrechender Innovationen in Red Teaming Abläufe.
In Kooperation mit dem Center for the Long View (CLV), dem Deloitte Center of Excellence für Szenarioplanung, kann eine zukunftssichere Szenarioanalyse möglicher Bedrohungslagen („Threat Landscapes“) stattfinden. Mögliche Szenarien werden durch das CLV-eigene AI-Tool Gnosis, kontinuierlich und langfristig überwacht.

Durch die Einbindung des Deloitte Neuroscience Institutes können mit neurowissenschaftlichen Methoden wie Eye-Tracking oder dem Messen von Gehirnströmen die Einflüsse unbewusster Prozesse auf die Entscheidungsfindung besser verstanden und daraus relevante Maßnahmen abgeleitet werden.

In Zusammenarbeit mit dem Deloitte Analytics Institute, dem Deloitte Kompetenzzentrum für Analystics, kann das Red Team auf zusätzliche Datenanalysen und interaktive Datenvisualisierung zurückgreifen und so komplexe Datenfelder, wie Big Data Analytics, aktiv in die Stärkung Ihrer Resilienz einbringen.

Durch den Einbezug dieser und anderer Expertenzentren wird das Red Team effektiv verstärkt und bietet Ihnen so ein komplett abgerundetes Servicepaket aus einem Haus.

Wie können wir Ihr Unternehmen am besten unterstützen? Um zu beurteilen, wie wir Sie bei der systematischen Erhöhung Ihrer organisatorischen Resilienz durch Red Teaming unterstützen können, bieten wir Ihnen folgende nächste Schritte an:

1

Im Rahmen eines halbtägigen Workshops stellen wir Ihnen unser Red Teaming Konzept detailliert und persönlich vor. Danach nehmen wir im Rahmen eines strukturierten Interviews mit Ihnen eine Einschätzung Ihrer aktuellen Situation vor. Wir betrachten dabei – angelehnt an die maßgeblichen Standards – Ihre Sicherheitskonzepte, -prozesse und -organisation – Ihre Analyse und Bewertung von Sicherheitsrisiken sowie den Stand Ihrer Trainings- und Ausbildungsmaßnahmen.

2

Auf dieser Basis geben wir Ihnen eine erste Einschätzung Ihrer gegenwärtigen Resilienz und diskutieren gemeinsam mit Ihnen die Verbesserungsmöglichkeiten.

3

Wir erstellen Ihnen ein individualisiertes Angebot, mit dem wir die identifizierten Handlungsfelder durch einen abgestimmten und fortlaufenden Einsatz unserer vier Services (Intel Service, Red Team Tests, War Games, Resilience Training) adressieren.

Kontakt

Katrin Rohmann
Partner, Strategic Risk & Public Sector Lead
Tel: +49 (0)30 2546 8127
krohmann@deloitte.de

Peter J. Wirnsperger
Partner, Head of Cyber Risk
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Knut Schönfelder
Senior Manager Cyber Risk, Head of Red Team
Tel: +49 (0)40 32080 4447
kschoenfelder@deloitte.de

Welche Fragen haben Sie zum Red Team Service?

Wir stehen Ihnen gern zur Verfügung.

Mehr Informationen finden Sie auf unserer Website www.deloitte.com/de

Deloitte.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen des Einzelfalls gerecht zu werden, und ist nicht dazu bestimmt, Grundlage für wirtschaftliche oder sonstige Entscheidungen zu sein. Weder die Deloitte GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited, noch ihre Mitgliedsunternehmen oder deren verbundene Unternehmen (insgesamt das „Deloitte Netzwerk") erbringen mittels dieser Veröffentlichung professionelle Beratungs- oder Dienstleistungen. Keines der Mitgliedsunternehmen des Deloitte Netzwerks ist verantwortlich für Verluste jedweder Art, die irgendjemand im Vertrauen auf diese Veröffentlichung erlitten hat.

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL"), eine „private company limited by guarantee" (Gesellschaft mit beschränkter Haftung nach britischem Recht), ihr Netzwerk von Mitgliedsunternehmen und ihre verbundenen Unternehmen. DTTL und jedes ihrer Mitgliedsunternehmen sind rechtlich selbstständig und unabhängig. DTTL (auch „Deloitte Global" genannt) erbringt selbst keine Leistungen gegenüber Mandanten. Eine detailliertere Beschreibung von DTTL und ihren Mitgliedsunternehmen finden Sie auf www.deloitte.com/de/UeberUns.

Deloitte erbringt Dienstleistungen in den Bereichen Wirtschaftsprüfung, Risk Advisory, Steuerberatung, Financial Advisory und Consulting für Unternehmen und Institutionen aus allen Wirtschaftszweigen; Rechtsberatung wird in Deutschland von Deloitte Legal erbracht. Mit einem weltweiten Netzwerk von Mitgliedsgesellschaften in mehr als 150 Ländern verbindet Deloitte herausragende Kompetenz mit erstklassigen Leistungen und unterstützt Kunden bei der Lösung ihrer komplexen unternehmerischen Herausforderungen. Making an impact that matters – für rund 286.000 Mitarbeiter von Deloitte ist dies gemeinsames Leitbild und individueller Anspruch zugleich.