WIE GEFÄHRLICH SIND SICHERHEITSLÜCKEN FÜR IHR NETZ?

Ein Diskussionspapier für IT-Führungskräfte aus dem Bereich Transport und Logistik

CGI

Experience the commitment®

SICHERHEIT – EINE WICHTIGE VORAUSSETZUNG FÜR DAS ÖKOSYSTEM TRANSPORT

Das Transportwesen ist ein wesentlicher Teil der nationalen Infrastruktur. Die Transportunternehmen haben die wichtige Aufgabe, die Integrität, Vertraulichkeit und Verfügbarkeit von Informationen und Leistungen zu sichern.

Diese Herausforderung wächst mit dem Angebot von intelligenten Transportsystemen und-services (ITS) wie vernetzten Autos, vernetzten Flugzeugen, automatisierten Fahrgast-Reiseinformationen und Selbstbedienungsterminals an Flughäfen. Durch die Online- Nachverfolgung von Frachtbewegungen und Fahrgästen wird diese Situation noch verschärft.

Dass sich diese Services immer mehr etablieren, beruht auf einer veränderten Infrastruktur und dem zunehmenden Einsatz von Cloud-Computing und Shared Services. Mit ihnen steigt jedoch auch das potenzielle Geschäftsrisiko.

Für Menschen, die schwere Störungen verursachen, wirtschaftlichen Schaden anrichten und die Sicherheit beeinträchtigen wollen, stellen Transportsysteme ein attraktives Ziel dar. Denn Transportsysteme sind von Natur aus anfällig für Angriffe. Schließlich handelt es sich um offene Systeme, bei denen zu vorhersehbaren Zeiten und an vorhersehbaren Orten viele Menschen zusammenkommen.

Die Studie Lloyd's Risk Index 2013 Global CXO[1] kam zu dem Ergebnis, dass die Computer- und Netzsicherheit mittlerweile zu den drei wichtigsten Themen in der Unternehmensführung gehört. Wenn Sicherheitslücken unerkannt bleiben und Sicherheitskontrollen unzureichend sind, kann dies das Geschäft und das gesamte Transportnetzwerk beeinträchtigen.

Kommen physische Angriffe und Cyberattacken zusammen, stellt dies für jedes Unternehmen eine echte Bedrohung dar. Diese sollten darauf entsprechend vorbereitet sein und sich Fragen stellen wie:

- Wie gut ist unser Unternehmen gegen solche Angriffe geschützt? Kann es einer Cyberattacke standhalten?
- Wie sicher sind unsere Unternehmensprozesse?
- Wie sicher sind die Netzwerke unserer Lieferanten und Partner?

Im Folgenden untersuchen wir, welche Risiken die neue Entwicklung für den Transportsektor mit sich bringt. Dabei kommen wir auch auf diese und weitere Fragen zurück.

[1]Lloyd's Risk Index 2013 basiert auf einer weltweiten Befragung von über 500 Führungskräften und Vorstandsmitgliedern, durchgeführt von Ipsos MORI für Lloyd's im April und Mai 2013: http://www.lloyds.com/news-and-insight/risk-insight/lloyds-risk-index

TRANSPORT HEUTE

Wenn wir auf der Straße, auf Schienen, per Schiff, im Flugzeug oder auch einfach nur zu Fuß unterwegs sind, möchten wir uns sicher fühlen. Regierungen, Verkehrsunternehmen, Transportdienstleister und andere Organisationen setzen alles daran, diese Sicherheit zu gewährleisten. Wir unterstützen sie dabei.

Für eine gut funktionierende moderne Gesellschaft ist es wichtig, Menschen und Güter gefahrlos transportieren zu können. Die Transportsysteme müssen daher so intelligent gestaltet sein, dass die Risiken verringert werden, ohne dass die Bewegungsfreiheit eingeschränkt wird. Für viele Unternehmen der Transportbranche ist entscheidend, dass ihre Kunden während des gesamten Kontakts positive Erfahrungen mit ihnen machen. Um diese Kundenerfahrung mit der unternehmenseigenen Strategie zur Risikominderung in Einklang zu bringen, werden Kameras, Scanner und andere Geräte zum Aufspüren und Durchleuchten von Gegenständen und Personen eingesetzt. In einer nächsten Stufe führen die Unternehmen zusätzliche Sicherheitsbewertungen durch – je nach eigenem Risikoprofil und Risikobereitschaft.

Das vorliegende Dokument beschäftigt sich mit den veränderten Bedingungen für Transportsicherheit und -risiko. Fast täglich wird in diesem Zusammenhang von neuen Vorfällen und Ereignissen berichtet. Schon allein aus diesem Grund sehen Unternehmen die Transportsicherheit nicht mehr als eines von vielen relevanten Themen an. Zählten Netzsicherheit und physische Sicherheit früher noch zum Routineprogramm, so haben sie heute oberste Priorität im Transportwesen. Unternehmen können es sich einfach nicht leisten, die Sicherheit im Transport-Ökosystem zu beeinträchtigen.

Auf den nächsten Seiten haben wir für Führungskräfte und Entscheidungsträger aus aller Welt Einblicke, Überlegungen und Analysen zusammengestellt, die die aktuelle Bedeutung von Transportsicherheit aufzeigen.

CGI im Bereich Sicherheit

CGI unterstützt Kunden bei der Einstufung von Bedrohungen und Risiken im Internet, beim Schutz ihrer geschäftlichen Interessen und beim sicheren Betrieb. Dabei verfolgen wir immer einen businessfokussierten Ansatz.

Unsere Experten arbeiten sehr intensiv an Gemeinschaftsprojekten mit dem Militär und den Geheimdiensten sowie an länderübergreifenden Verteidigungsprogrammen, die im Fokus der Öffentlichkeit stehen. Sie schützen Regierungsnetz werke, wichtige Infrastrukturen und das geistige Eigentum von Unternehmen tagtäglich vor 43 Millionen raffinierter Angriffe.

Wir haben mehr als 9.000 Biometriesysteme und -geräte an über 100 Standorten weltweit implementiert und unterstützt. Diese liefern jährlich mehr als vier Millionen biometrische Eintragungen für das US-Militär.

Schreckminuten auf dem Flughafen von Los Angeles

Im April 2013 konnten die Passagiere am Flughafen in Los Angeles fünf Minuten lang auf den Anzeigetafeln folgende Meldung lesen: „Notfall – verlassen Sie das Terminal!“ Zunächst wurde hinter der Nachricht ein Hackerangriff vermutet. Später erklärten die Verantwortlichen des Flughafens, dass es sich um den Mitarbeiter eines Vertragspartners handelte. Dieser verfügte über eine Zugriffsberechtigung und hatte das Überschreiben der Bildschirme versehentlich ausgelöst.

Angriff auf die Website von KLM

Am 18. April 2013 um 11 Uhr traten auf der Website von KLM erstmals Probleme auf. Weder der Online-Check-in noch die Buchung von Flugtickets oder sonstige Informationsdienste funktionierten. Die Ursache war ein Denial-of-Service-Angriff. Erst nach zwei Tagen, am 20. April, funktionierten die Dienste wieder normal.

TRENDS UND RISIKOFAKTOREN

IM BEREICH REISEN UND TRANSPORT HAT DIE ZUKUNFT SCHON BEGONNEN. SIND WIR BEREIT DAFÜR?

Der technologische Fortschritt hat automatisierte, selbstfahrende Autos hervorgebracht, vernetzte Flugzeuge und fahrerlose Züge. Doch die Weiterverbreitung dieser Technologien verzögert sich, weil die Menschen an der Zuverlässigkeit zweifeln und komplexe Rechtsvorschriften eingehalten werden müssen.

Die Wertschöpfungskette in allen Teilen zu sichern, bedeutet einen Balanceakt – zwischen Kosteneffizienz, neuen Technologien und Compliance. Unternehmen und Verantwortliche im Bereich Sicherheit und Informationstechnologie erkennen genau hier das Gefahrenpotenzial von zunehmenden Cyberangriffen und physischen Attacken.

Eine Verbesserung des Erlebnisses für den Fahrgast sollte nicht zur Erhöhung der Risikofaktoren führen. Allerdings wird zunehmend klar, dass die Risiken nicht mehr nur von einzelnen Hackern ausgehen, die auf der Suche nach anfälligen Websites, Hintertüren oder schädlicher Software sind. Jeden Tag berichten Medien darüber, wie weit Organisationen und kriminelle Vereinigungen gehen, um durch gezielte Angriffe an Informationen zu gelangen.

Schätzungen zufolge können gezielte Angreifer durchschnittlich 416 Tage innerhalb eines Unternehmens aktiv sein, bevor sie entdeckt werden.[2] Solche gezielten Angriffe auf Unternehmen haben weitreichende Konsequenzen für die Marke, den Ruf und die betrieblichen Abläufe. Sony büßte beispielsweise über Nacht 6 % seiner Marktanteile ein: Die Konsumenten hatten aufgrund einer Sicherheitsverletzung, bei der vertrauliche Kundendaten abhanden kamen, ihr Vertrauen in das Unternehmen verloren. Vermutlich hat die Mehrheit der global tätigen Unternehmen bereits Datenverluste in irgendeiner Form erlitten. Datenmissbrauch kostet Unternehmen Millionen von Euro. Wäre ein Unternehmen des öffentlichen Verkehrs in der Lage, sich von einem solchen Reputationsverlust zu erholen, selbst wenn die Sicherheit seines Netzwerks bewahrt würde?

[2]Mandiant – M-Trends 2012: https://www.mandiant.com/news/release/mandiant-releases-annual-threat-report-on-advanced-targeted-attacks/Transport Security

WAS HEISST DAS FÜR UNTERNEHMEN?

Wenn ein Unternehmen das Risikoprofil seiner Schwachstellen nicht überprüft und aktualisiert, so drohen eine Rufschädigung und Schlimmeres. Die Wahrscheinlichkeit eines Vorfalls und die Auswirkungen auf die Infrastruktur und die Services eines Unternehmens müssen dabei unbedingt in Betracht gezogen werden. Kann das Unternehmen eine Krise erfolgreich bewältigen und überstehen? Wie lange dauert es, bis

- ein nicht funktionierendes Gepäcksystem den reibungslosen Ablauf auf einem betriebsamen internationalen Flughafen stört?
- die Sperrung eines Systems aus Hauptverkehrsadern zu Staus führt?
- ein Terroranschlag oder Gewaltakt eine Krisensituation auslöst?
- man das Vertrauen seiner Kunden, sein Markenimage und seinen Ruf verliert?

Wenn Organisationen nicht die Eintrittswahrscheinlichkeit einer Bedrohung, deren Auswirkungen auf ihr Geschäft und eine Strategie zur Risikominderung thematisieren, dann beschäftigen sie sich auch nicht damit, welchen Einfluss dies auf ihre Marke und ihren Gewinn haben könnte.

Die Vernetzung unserer Transportsysteme nimmt zu: Fahrgastinformationssysteme in Echtzeit und Mobile Ticketing sind bereits heute weit verbreitet. Gemäß den Regierungsinitiativen für offene Daten werden viele dieser Informationen zugänglich gemacht, damit Drittentwickler sie zusammenstellen können und so vorausschauende Analysen zu Verbraucherentscheidungen, Frachtmustern etc. möglich machen. Doch wir stehen erst am Anfang der Vernetzung. Mit neu entwickelten Anwendungen für mobile Endgeräte und dem Internet of Things ist eine isolierte Sicherheitsstrategie nicht mehr zeitgemäß. Auch wenn man es bis vor kurzem noch nicht für nötig hielt, sich über die sichere Aktualisierung von Fahrzeugelektronik über das Funknetz Gedanken zu machen: Schon heute sind viele unserer Automobile vernetzt; 2030 sollen autonome Kraftwagen auf unseren Straßen zum normalen Erscheinungsbild gehören. In der Tat stehen wir kurz vor der Produktionsreife einer ganzen Reihe von vernetzten Fahrzeugen. Aus diesem Grund denken die Transportbehörden auch bereits darüber nach, wie Einsatzzentralen des Verkehrsmanagements einen größeren Einblick in die Verkehrsbewegungen erhalten können. Wie lassen sich z. B. Fahrzeuge in der Umgebung eines Krankenhauses mit Hitzestau kontrollieren, um die Abgasemissionen zu reduzieren? Wie kann man Autos im Falle eines Unfalls automatisch umleiten? Wie lassen sich in Hauptverkehrszeiten die Fahrzeuggeschwindigkeiten automatisch verringern? Zur Steuerung könnten z. B. personalisierte Mikronavigationsanfragen an die Streckenführungssysteme der Fahrer eingesetzt werden. Viele weitere Lösungen befinden sich in der Entwicklung. Doch diese Anwendungen könnten auch durch einen verärgerten Mitarbeiter oder einen Terroristen gestört werden.

Tricks zum Hacken von Autos auf der Hackerkonferenz in Las Vegas aufgedeckt

Auf der 21. DEFCON präsentierten Charlie Miller, Sicherheitsingenieur bei Twitter, und Chris Valasek, Leiter des Bereichs Security Intelligence bei IOActive, ihre selbst entwickelten Werkzeuge zum Hacken computergestützter Funktionen eines 2010 Toyota Prius und eines 2010 Ford Escape. Sie demonstrierten, wie einfach die Alarmsysteme der Autos deaktiviert und andere Geräte mit GSM- und mobilen Verbindungen gesteuert werden können.

Erreicht wurde dies mit einem direkten Angriff: Nach dem Anschließen eines Laptops an das Kommunikationsnetzwerk der Motorsteuerung speisten Charlie Miller und Chris Valasek negative Signale ein. Dadurch konnten sie unter anderem die Fahrzeugbremsen während der Fahrt deaktivieren, ruckartige Bewegungen am Lenkrad hervorrufen, das Fahrzeug beschleunigen, den Motor abwürgen, den Gurt schnell anziehen, falsche Werte auf der Geschwindigkeits- und der Tankanzeige erscheinen lassen, die Fahrzeugbeleuchtung an- und ausschalten und die Hupe auslösen.

Die Forscher fanden außerdem einen Weg, anhaltende Angriffe zu orten. Durch die Modifizierung der Motorsteuerungssoftware werden negative Signale selbst dann gesendet, wenn keine physische Verbindung mehr zu den Steuerungseinheiten besteht. Auch hierfür war zunächst ein direkter Zugang zum Fahrzeug erforderlich. 2011 fand jedoch eine Forschungsgruppe des Centre for Automotive Embedded Systems Security heraus, dass mithilfe eines CD- oder USB-Spielers und des Bluetooth- bzw. Mobilfunknetzes eine Reihe ferngesteuerter Angriffe in einem Auto ausgeführt werden kann. Was, wenn diese direkten und ferngesteuerten Methoden erfolgreich kombiniert werden?

Bay Area Rapid Transit Ziel eines Hackerangriffs

Im August 2011 griff die Gruppe Anonymous Hackers die Website myBART.org des Bay Area Rapid Transit (BART) von San Francisco an. Die Attacke ereignete sich, nachdem BART den Mobiltelefonservice gesperrt hatte, um damit einen Protest in der vorangegangenen Woche zu stoppen. Die Hacker verunstalteten die Website mit den Logos von Anonymous Hackers und veröffentlichten persönliche Kontaktdaten von mindestens 2.400 Nutzern der Seite, einschließlich Namen, Passwörtern, E-Mail-Adressen, Postanschriften und Telefonnummern.

Schwachstellen der Infrastruktur aufgedeckt

2008 ließ ein Teenager mithilfe einer umgerüsteten Fernbedienung zur Steuerung von Schaltpunkten in Łódź, Polen, eine Straßenbahn entgleisen. Zwölf Personen wurden verletzt. Die veraltete Infrastruktur der Bahn nutzte ein Infrarot-Steuersystem, das in keiner Weise gesichert war.

ZUSAMMENPRALL DER REALEN UND DER VIRTUELLEN WELT

Der Zusammenprall der realen und der virtuellen Welt macht die Absicherung des Transportsektors nicht einfacher – auch in Bezug auf Kundenerlebnis, Kundenreise und den Umgang mit der Fracht. Die Gefährdung der Infrastruktur und ihre Konsequenzen müssen stärker berücksichtigt werden. Dies bedeutet auch, dass die Prozesse die Angriffe und deren Folgen besser abbilden müssen. In puncto Risikominderung und Unternehmensentwicklung ist daher visionäres Denken gefragt.

Die größte Gefahr, auf die sich Transportunternehmen derzeit vorbereiten, besteht in einer Kombination aus physischen Angriffen und Cyberattacken auf ihre Infrastrukturen. Viele Unternehmen versuchen, diesen Risikofaktor mit Risikoregistern in den Griff zu bekommen. Mehr und mehr Social-Media-Anwendungen, Online-Technologien und Selbstbedienungsterminals verstärken die Gefahr zusätzlich. Die daraus resultierende Matrix zur Risikominderung muss daher die folgenden Aspekte berücksichtigen:

MOTIVE, TÄTER UND ANGRIFFE

- Beabsichtigt und geplant: Demonstrant, Terrorist, Krimineller, verärgerter Fahrgast, Mitarbeiter oder Dritter
- Beabsichtigt und spontan: opportunistischer Krimineller, verärgerter Fahrgast, ehemaliger Mitarbeiter oder Dritter
- Bösartig und unspezifisch: Malware, Hacken, Spoofing
- Bösartig und spezifisch: gezielter Angriff auf ein Unternehmen, den Industriesektor oder das Ökosystem
- Umweltbedingt: Wetter, Stromausfall, höhere Gewalt
- Zufällig: unbeabsichtigte Folgen

ART DES ANGRIFFS, ANGRIFFZIELE

- Physischer Zugriff
- Schnittstellen
- Cyberangriffe: Malware aus dem Internet
- WLAN
- Denial of Service
- Beeinträchtigung der Transport-sicherheitseinrichtungen

POTENZIELLE FOLGEN

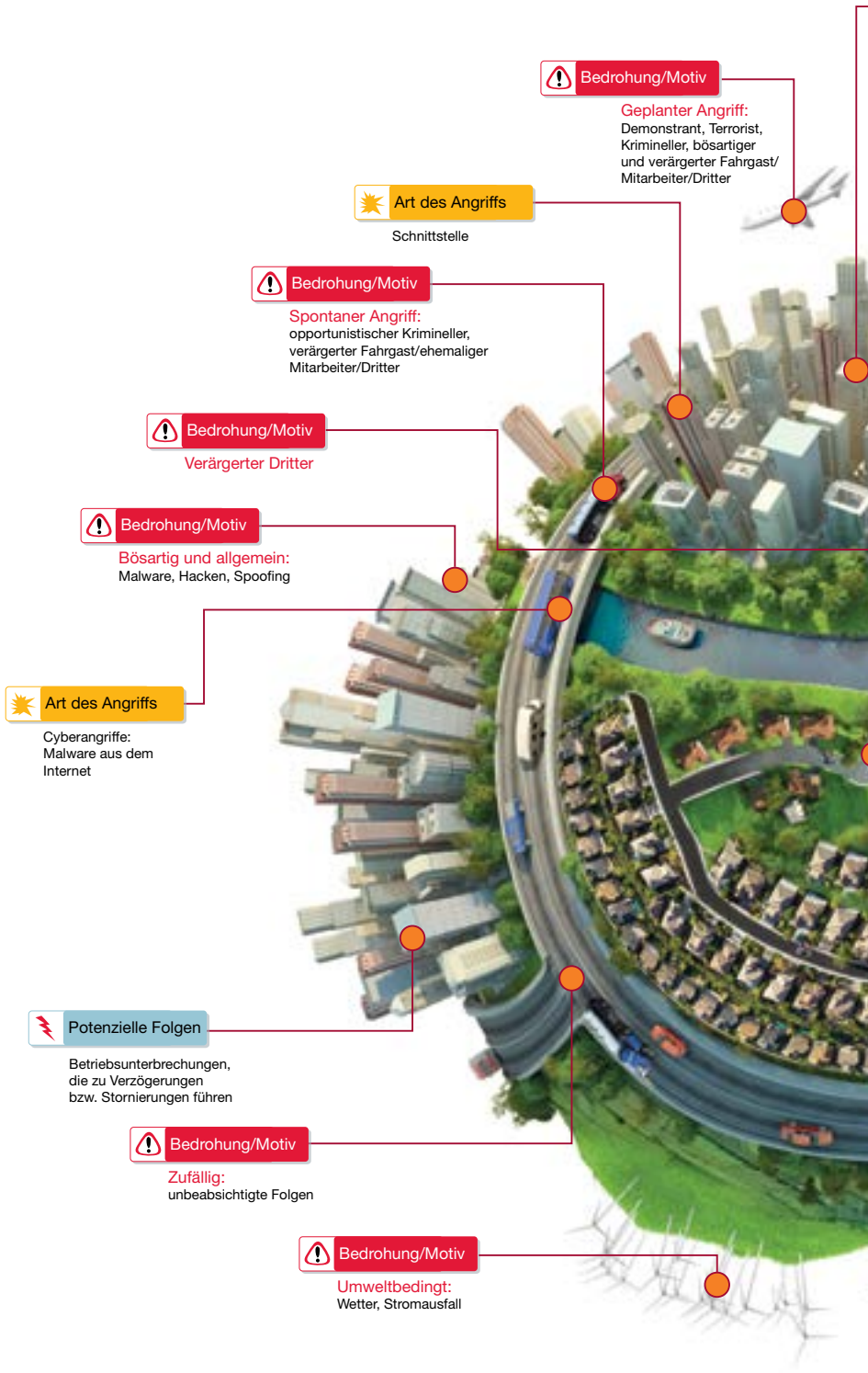
- Einfluss auf Informationen, Vertraulichkeit, Integrität oder Verfügbarkeit
- Ausfall der IKT (Informations- und Kommunikationstechnik)
- Unterbrochener Betrieb, der zu Verzögerungen bzw. Stornierungen führt
- Einschränkungen für Fahrgast oder Fracht
- Schädigung des Rufs und der Marke
- Falsche geladene Fracht oder falsch zugestiegene Fahrgäste, Transport zum falschen Zielort
- Verstoß gegen die zugrundeliegenden Sicherheitsvorschriften

Krisenmanagementszenarien müssen nicht nur Angriffe auf die direkte Infrastruktur des Unternehmens, sondern auch solche auf das gesamte Transportsystem berücksichtigen. Vorfälle wie Vulkanaschewolken, Brände auf Flughafenlandebahnen und Unfälle von Hochgeschwindigkeitszügen machen deutlich, dass in solchen Situationen umgehend und effektiv gehandelt werden muss.

Doch wann wird aus einem Vorfall eine handfeste Krise? Und wie handhaben Unternehmen Ereignisse in- und außerhalb ihres Einflussbereichs? Wie zuvor bereits angesprochen, berichtete Mandiant[3], dass Angreifer bis zu 416 Tage in der Infrastruktur eines Unternehmens aktiv sein können, bevor sie entdeckt werden. Um das Risiko zu verkleinern, muss diese Zahl verringert und der Angreifer fast augenblicklich aufgespürt werden. Außerdem ist es nicht mehr ausreichend, nur die eigene Umgebung zu sichern. Doch wie lässt sich ausschließen, dass bei Wettbewerbern und Drittanbietern Sicherheitslücken bestehen?

[3]Mandiant – M-Trends 2012: https://www.mandiant.com/news/release/mandiant-releases-annual-threat-report-on-advanced-targeted-attacks/Transport Security

DROHENDE GEFAHREN BEIM ZUSAMMENPRALL DER REALEN UND DER VIRTUELLEN WELT




Art des Angriffs
Beeinträchtigung der Transportsicherheitseinrichtungen
Art des Angriffs
Kombination aus physischen Angriffen und Cyberattacken
Potenzielle Folgen
Ausfall der IKT (Informations- und Kommunikationstechnik)
Bedrohung/Motiv
Beabsichtigter Angriff:
Spezifischer oder gezielter Angriff auf ein Unternehmen, den Industriesektor oder das Ökosystem
Art des Angriffs
Denial of Service
Potenzielle Folgen
Schädigung des Rufs und der Marke
Art des Angriffs
WLAN
Potenzielle Folgen
Einschränkungen für Fahrgast/Fracht
Art des Angriffs
Physischer Zugriff
Bedrohung/Motiv
Verärgerter Mitarbeiter
Potenzielle Folgen
Einfluss auf Informationen, Vertraulichkeit, Integrität oder Verfügbarkeit
Art des Angriffs
Gefährdung durch Dritte

Das größte ITS-Projekt der Welt

Saudi-Arabien hat eine Bevölkerung von 27 Millionen Menschen. Jeden Tag gibt es 18 tödliche Unfälle. Pro Kopf gesehen sind das fünfmal mehr als in Europa.

Das Programm ATVAM (Automated Traffic Violations Administering and Monitoring) umfasst die acht größten Städte des Königreichs. Es dient dazu, die Sicherheit auf den Straßen zu erhöhen, die Strafverfolgung zu erleichtern und das Stauaufkommen durch ein besseres Verkehrsmanagement zu senken.

Das Königreich wurde dazu in drei Regionen aufgeteilt, die unserer Programmverwaltung Bericht erstatten. Das Programm stellt mehrere tausend Straßensysteme zur Verfügung. Dazu zählen Kfz-Nummernschild-Sensoren und intelligente Überwachungssysteme ebenso wie fest installierte und mobile Geschwindigkeits- und Rotlichtüberwachungsanlagen. Ein Dutzend Kommando- und Einsatzzentralen bündelt die Sicherheits- und Verkehrsmanagementfunktionen und macht auf Regelverstöße aufmerksam.

Dies zeigt, dass ITS-Systeme auch den großen Herausforderungen in Saudi-Arabien gewachsen sind. Sie können hier ebenso erfolgreich eingesetzt werden wie an anderen Orten. Die Messlatte für echte Systemintegration liegt in Zukunft weltweit noch höher.

VORBEUGUNG – SICHERHEIT UND GARANTIE

Mit Methoden zur Berechnung von Risikowahrscheinlichkeit und -behandlung bekommen Organisationen ein Rahmenkonzept an die Hand, mit dem sie Risiken minimieren können: Es besteht garantierte Sicherheit vor gegenwärtigen und zukünftigen Risiken. Ob es nun um vernetzte Autos geht oder Last-Mile-Paketauslieferungen – unsere Transport- und Logistiksysteme müssen widerstandsfähig sein und geschützt werden.

In ähnlichen Gemeinschaftsprojekten mit Organisationen wie British Airways oder einem großen Eisenbahnunternehmen in Großbritannien haben wir Kernkomponenten festgelegt und sichergestellt, dass jeder Bereich auf Schwachstellen überprüft wird. Dazu bewerteten wir die Cyberrisiken und wandten die von unseren internationalen Security Operation Centres gesammelten Informationen auf die externen Internetschwachstellen jeder Organisation an.

Seit über 30 Jahren entwickeln wir unsere Methoden und Herangehensweisen kontinuierlich weiter. Das Projekt CESG CHECK wurde von unserem Expertenteam für Penetrationstests ins Leben gerufen und bekam jetzt grünes Licht. Unser Team besteht aus hochqualifizierten Sicherheitsberatern, die sich auf Penetrationstests/ Schwachstellenanalysen spezialisiert haben. Sowohl Teamleiter als auch Teammitglieder sind für CESG CHECK qualifiziert.

UNSERE HAUPTZIELE FÜR DIE GARANTIERTE SICHERHEIT

- Mit der größtmöglichen garantierten Sicherheit aufzeigen, ob ein System für bestimmte Sicherheitsschwachstellen anfällig ist oder nicht
- Eindeutige Empfehlungen zur Verringerung von Sicherheitslücken aussprechen, die sich einfach umsetzen lassen und an die Systemanforderungen angepasst sind
- Die Lösung validieren und das schwächste Glied hinsichtlich der Sicherheit ermitteln
- Die Sicherheit der zugrundeliegenden Software mittels SilverKite, der IPR-Lösung von CGI, gewährleisten

CGI wird vom Department of Homeland Security ausgewählt

Das Department of Homeland Security (DHS) und die United States Coast Guard (USCG) haben mit CGI einen unbegrenzten ID/IQ-Vertrag (Indefinite Delivery/ Indefinite Quality) für Technik, Beschaffung und Unterstützungsdienste für Unternehmen abgeschlossen (TABSS). TABSS spielt für die erfolgreiche Unterstützung der Planung und Verwaltung von Programmen, Projekten und wichtigen Anschaffungen eine zentrale Rolle. So hilft TABSS, die Ziele des DHS zu erfüllen und das Wohlergehen des Landes zu sichern.

CGI fokussiert sich auf Aufträge im Bereich erfolgskritischer Ingenieursleistungen, Programmmanagement und technischer Services über den gesamten Lebenszyklus hinweg – von der Initiierung über Forschung, Entwicklung und Produktion bis hin zu Einsatz, Betrieb, Upgrade und Bereitstellung von DHS-Programmen und der dafür benötigten Ressourcen. Durch unsere Fachkompetenz und unsere zukunftsorientierten Lösungen steigern wir die Einsatzfähigkeit und Kosteneffizienz des DHS.

NS gewinnt Kontrolle über die gesamte Fahrgastinformationskette

CGI unterstützte das niederländische Eisenbahnunternehmen NS bei der proaktiven Verwaltung seiner Informationskette. NS ist nun in der Lage, Sachverhalte zu klären, bevor sie zum Problem werden, sich ein einheitliches Bild von der gesamten Informationskette zu machen, bestimmte Abschnitte fokussiert zu betrachten und Probleme schneller zu lösen.

CGI im Transportwesen

CGI arbeitet mit Transport- und Logistikunternehmen zusammen, um die Effizienz zu steigern, innovative Angebote auf den Markt zu bringen und das Fahrgasterlebnis insgesamt zu verbessern.

Derzeit sind wir für über 200 Kunden tätig und stellen IT-Komplettlösungen für Dienstleistungen im Transport- und Logistikbereich zur Verfügung – von der Beratung bis hin zum vollständigen IT-Outsourcing und zu spezialisierten IT- und Sicherheitsdienstleistungen.

In den 30 Jahren unserer Tätigkeit in dieser Branche haben wir:

- für Lufthansa automatische Check-in-Terminals am Gate eingeführt
- PCI-DSS-konforme Dienstleistungen für Shell-Tankkarten durchgeführt
- technische Sicherungen am Flughafen Gatwick bereitgestellt
- den PCI für das Programm Barclays Cycle Hire von Transport for London realisiert
- die Einführung der ersten biometrischen Grenzkontrolle in Europa unterstützt
- Sicherheits- und Penetrationstests für Bahnbetreiber durchgeführt
- BMW Dienstleistungen zum Sicherheitsmanagement bereitgestellt
- Software zur Unterstützung der Verwaltung von zehn Flughäfen in Portugal geliefert

WIR VERSTEHEN DIE ANFORDERUNGEN IM BEREICH REISE, TRANSPORT UND SICHERHEIT

CGI hat Lösungen für die Transportsicherheit entwickelt, um eine komplexe Aufgabenstellung zu vereinfachen. Damit tragen wir dazu bei, Passagiere, Fracht und risikobehaftete Vermögenswerte besser vor all denjenigen zu schützen, die ihnen schaden möchten. Dafür arbeiten wir Seite an Seite mit Regierungen auf der ganzen Welt, mit dem Militär und Strafverfolgungs- bzw. Sicherheitsbehörden. Dazu kooperieren wir mit der Luftfahrt-, Schifffahrts- und Eisenbahnindustrie sowie mit öffentlichen Behörden, um:

- beste Kundenerfahrung zu ermöglichen
- Werte zu schöpfen und die Effizienz zu steigern
- die Reputation zu wahren und zu verbessern
- ein starkes Umwelt-, Gesundheits- und Sicherheitsprogramm zu erstellen, das den Sicherheitsanforderungen in vollem Umfang entspricht
- Compliance und Governance zu überprüfen
- die Sicherheitsmaßnahmen von Organisationen innerhalb ihres weiterreichenden Ökosystems zu untersuchen
- neue Technologien wie die Cloud und mobile Apps einzusetzen und dabei die Sicherheitsrisiken und Auswirkungen auf das Unternehmen zu berücksichtigen
- die Vertraulichkeit der Daten von Mitarbeitern, Kunden und Auftraggebern sicherzustellen
- die Kosten der Reputation und die Kapitalkosten zu überprüfen
- die Reputationsrisiken und den Vertrauensverlust bei Kunden zu untersuchen
- die finanziellen Kosten eines Krisenmanagements zu untersuchen
- den Grad der Bedrohung einzuschätzen
- die vorhandenen Gegenmaßnahmen zu untersuchen
- Strategien zur Handhabung dieser Bedrohungen vorzuschlagen
- vorausschauende Analysen der Bedrohungsvektoren sowie Gegenmaßnahmen zu bieten
- eine Überwachung rund um die Uhr bereitzustellen
- die Kontinuität der Betriebsabläufe zu schützen und sicherzustellen

SICHERE PROJEKTRESSOURCEN UND LANGJÄHRIGE ERFAHRUNG IM TRANSPORT- UND LOGISTIKSEKTOR

Wir sind seit über drei Jahrzehnten erfolgreich in der Transport- und Logistikbranche tätig. Wir unterstützen unsere Kunden weltweit dabei, ihre betriebliche Effizienz zu steigern und Verbesserungen in puncto Sicherheit zu erzielen. Zu unseren Kunden zählen große Flughäfen wie London Heathrow, Gatwick Airport, Amsterdam Airport Schiphol und Aeroportos de Portugal. Andere wichtige Unternehmen, mit denen wir im Luftverkehrssektor eng zusammenarbeiten, sind CAA und Fluggesellschaften wie Air Canada, Lufthansa, Air France/KLM und Finnair. Zu unseren Partnern in der Schienenverkehrsindustrie gehören Via Rail, ProRail, Network Rail, Queensland Rail, Deutsche Bahn sowie STM und AMT in Montreal. Auch Automobilherstellern wie BMW, KIA, Ford, Toyota, Jaguar und Land Rover sowie Flugzeugherstellern wie Rolls-Royce, Bombardier und Airbus stehen wir mit unseren Dienstleistungen zur Seite. Außerdem arbeiten wir beispielsweise in Schweden, Finnland und den Niederlanden mit den Transportministerien der Landesregierungen sowie mit Transportbehörden wie Transport for London, Transport for Greater Manchester, Translink in Vancouver und Caltrans zusammen.

FÜHRENDER PARTNER IN PUNCTO SICHERHEIT

Die Sicherheit gehört zu unserem Spezialgebiet – wir haben über 60 % der Sicherheitsbewertungen für die Regierung in Großbritannien durchgeführt und erstklassige Sicherheitslösungen für Regierungen und Blue-Chip-Organisationen in der ganzen Welt bereitgestellt. Seit über 30 Jahren ermöglichen wir unseren Kunden weltweit einen sicheren Arbeitsablauf im privaten und öffentlichen Sektor. Dabei verfolgen wir einen businessfokussierten Ansatz. Unser Team besteht aus über 1.200 Sicherheitsexperten. Mit unseren globalen Ressourcen leisten wir eine optimale Unterstützung unserer Kunden vor Ort.

Implementierung eines der weltweit größten Identitätsmanagementsysteme für BMW

Bei BMW arbeitete ein Benutzerkreis von 280.000 Mitarbeitern, Händlern und Zulieferern mit über 1.000 Anwendungen auf verschiedenen Plattformen, in unterschiedlichen Prozessen und Systemen. Aufgrund wachsender Geschäftsanforderungen wurden diese Systeme so komplex, dass sie im Laufe der Zeit nicht mehr tragbar waren: Die Kosten für Support und Instandhaltung wurden zu hoch. BMW wandte sich an CGI, um den gestiegenen Sicherheitsbedürfnissen und neuen internationalen Gesetzen auch in Zukunft entsprechen zu können.

Wir haben das neue ID-Managementsystem (IdAS) für BMW entworfen und umgesetzt. Darin wurden viele unterschiedliche Management- und Bereitstellungsprozesse integriert und der Flexibilitäts-, Sicherheits- und Geschwindigkeitsbedarf von BMW wurde automatisiert. IdAS wurde 2009 erfolgreich eingeführt. BMW-Kunden erhalten nun mehr Informationen von den Händlern, da diese direkt auf die Informationssysteme von BMW zugreifen können.

Großes Eisenbahnunternehmen erhöht Sicherheit

Wir haben die Sicherheit eines großen Eisenbahnunternehmens anhand von vier Stufen verbessert:

1. Entwicklung einer funktionalen Sicht bzw. eines Gesamtbildes – mit Ist- und Soll-Status der Organisation
2. Erstellung eines Profils bezüglich der Bedrohung aus dem Netz mithilfe interner und externer Datenquellen
3. Bereitstellung einer detail-lierten Analyse bestimmter Bereiche, z. B. Sicherheitspolitik, Telekommunikation, Risikomanagement, Sicherheitsmaßnahmen, SCADA, Signalsysteme und weitere wichtige Projekte und Systeme
4. Erarbeitung eines schriftlichen Berichts- und Optionspapiers, das die Möglichkeiten des Unternehmens für die zukünftige Ausweitung des Schutzes vor Internetbedrohungen aufzeigt; Übergabe des Berichts an das Team der Informationssicherheit und an wichtige Stakeholder; Start eines offiziellen Prozesses zur Überarbeitung und Rückmeldung; Bereitstellung neuer Informationen, Vereinbarung von Änderungen und Umsetzung des Berichts in der neuen Version

Unsere Services umfassen Beratungsdienstleistungen, Systems Integration und Managed Services. Wir wenden uns damit an die betreffenden Menschen und berücksichtigen Geschäftsprozesse ebenso wie technologische Aspekte. Wir haben ein einzigartiges Verständnis dafür entwickelt, wie die komplexen Anforderungen unserer Kunden an die Sicherheit erfüllt werden können und gleichzeitig die Geschäftsflexibilität erhalten, die betriebliche Effizienz verbessert und das Vertrauen der Kunden, Lieferanten, Stakeholder und Mitarbeiter gesteigert werden kann. Unsere internationalen Sicherheitsteams unterstützen viele der weltweit führenden Unternehmen. Dazu gehören: Barclaycard, Bombardier, BMW, Carrefour, Czech Post, Daimler, Department of Defence, Airbus (EADS), E.ON, die Europäische Weltraumorganisation, National Audit Office, Network Rail, Philips, Sagem, SAS, Scania, Shell, SNCF, Scottish and Southern Electric, T-Mobile und Transport for London.

Dazu werden viele wichtige nationale Infrastrukturen durch uns abgesichert. Unsere globale Methodik hilft Unternehmen wie Shell bei der Handhabung ihres Informationsrisikomanagements: So können sie die technologischen Herausforderungen von heute und morgen leichter bewältigen.

CGI GEHT VORAN

CGI denkt im Hinblick auf die Sicherheit immer einen Schritt weiter. So sind wir beispielsweise auch am Schutz des Satellitennavigationsprogramms Galileo beteiligt. Bei Galileo stellen wir für die Segmente Bodenkontrolle und Bodenmission die Sicherheits- und Hauptverwaltungseinrichtungen bereit.

Außerdem widmen wir uns dem heiklen Thema, ein Gleichgewicht zwischen rigorosen Sicherheitskontrollen, einem angenehmen Reiseerlebnis und einer zügigen Abwicklung des Boardings zu finden. Durch die Verknüpfung automatischer Schranken mit fortschrittlichen biometrischen Lesegeräten und Chipkarten haben wir automatisierte und biometrische Grenzkontrollen möglich gemacht. So können sich Reisende schnell und bequem auf Flughäfen oder zwischen verschiedenen Ländern bewegen, ohne dass die Sicherheit dadurch beeinträchtigt wird.

Die Biometrie zählt zu unseren Kernkompetenzen. Bei der Realisierung biometrischer Systeme sind wir einer der erfahrensten Anbieter weltweit. Unsere Systeme werden bereits in Fußballstadien, Einkaufszentren und an vielen anderen Orten eingesetzt, an denen sich sehr viele Menschen gleichzeitig aufhalten oder die einen hohen Grad an Sicherheit erfordern.

CGI

CGI GROUP INC.
de.cgi.com
cgi.com/cyber

Über CGI

Mit 68.000 Mitarbeitern an 400 Standorten in 40 Ländern übernimmt CGI vor Ort Verantwortung für den Erfolg seiner Kunden und bietet ihnen gleichzeitig globale Lieferfähigkeit. Seit unserer Gründung im Jahr 1976 pflegen wir eine strikte Lieferdisziplin, dank der unsere Projekte in Bezug auf Zeit- und Budgettreue in der Branche führend sind. Mit Business und IT Consulting, Systemintegration sowie Outsourcing Services auf höchstem Niveau unterstützt CGI seine Kunden dabei, laufende Investitionen besser zu nutzen und gleichzeitig neue Technologie- und Business-Strategien einzusetzen, mit denen sich optimale Lösungen für die gesamte Wertschöpfungskette erreichen lassen. Das Resultat unseres Commitments zeigt sich im gemessenen Kundenzufriedenheitswert, der in den vergangenen zehn Jahren durchgängig mehr als neun von zehn möglichen Punkten betrug.