November 2025

ComConsult GmbH
Beratung + Planung + Schulung

# Der Netzwerk Insider

## Ein Deepdive zu den Unterwasser-Datenautobahnen

**von Dr. Philpp Rüßmann**
Das Leben ohne das Internet ist für uns im Informationszeitalter nicht denkbar. Die Möglichkeit, schnell viele Daten von einem Ende der Welt zum anderen Ende zu übertragen, bestimmt unser alltägliches digitales Leben. Eine besondere Herausforderung stellt dabei die etwa 6.000 km lange Verbindung durch den Atlantik von Europa nach Amerika dar.

Seite 7

## Geordnete Kommunikation ist der Schlüssel zum guten Service

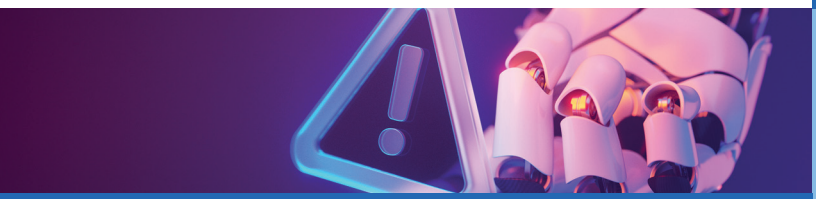
**von Dr. Behrooz Moayeri**
Kennen Sie jemanden, der sich über schlechten Service im IT-Bereich beschwert? Dann sind Sie nicht allein. Der IT-Service steht allgemein in einem schlechten Licht. Es liegt in der Natur des Menschen, Gutes zu vergessen und sich an Schlechtes zu erinnern.

Seite 2

## Prüfung von Ladekabeln für Elektroautos

**von Peter Steufmehl**
Das Ladekabel für Elektrofahrzeuge (EV, Electric Vehicle) ist mehr als ein einfacher Stromleiter. Es handelt sich um eine hochentwickelte, sicherheitsrelevante Systemkomponente, die eine kontinuierliche bidirektionale Kommunikation der Ladestation mit dem Elektrofahrzeug aufrechterhält, um den Ladevorgang präzise zu steuern und zu überwachen.

Seite 12



Webinar der Woche

## KI-Management aus der Informationssicherheitsperspektive

Seite 21

## Supply-Chain-Angriffe und ihre Auswirkungen

**von Dr. Markus Ermes**
Und wieder macht ein neuer erfolgreicher Cyberangriff Schlagzeilen: Unter Titeln wie „BER nach Cyberangriff lahmgelegt“ wurde in den letzten Wochen darüber berichtet, dass ein Angriff verschiedene Flughäfen in Deutschland lahmgelegt oder zumindest den Check-in für die Passagiere deutlich zeitaufwendiger gemacht hat. Was ist passiert? Zäumen wir das Pferd von hinten auf!

Seite 22

# Geordnete Kommunikation ist der Schlüssel zum guten Service

von Dr. Behrooz Moayeri

Kennen Sie jemanden, der sich über schlechten Service im IT-Bereich beschwert? Dann sind Sie nicht allein. Der IT-Service steht allgemein in einem schlechten Licht. Es liegt in der Natur des Menschen, Gutes zu vergessen und sich an Schlechtes zu erinnern. Zufriedene Kunden melden sich selten mit Lob, unzufriedene dafür umso mehr mit Klagen, das liegt in unserer Natur (oder Erziehung?). Weil Dienstleister keine neuen Menschen als Kunden schaffen können, müssen sie besser werden, um ihren Ruf zu retten.

## Eine wahre Geschichte

Alle sind im Leben von IT-Produkten weniger Weltkonzerne abhängig. Diese nutzen diese Abhängigkeit gnadenlos aus, um noch höhere Profite zu machen. Im besten Fall können sich diese Riesen einen schlechten Ruf leisten und die Probleme von Milliarden IT-Nutzern ignorieren. Kleine Dienstleister können das nicht.

Microsoft zwingt mit der Einführung von Windows 11 hunderte Millionen Kunden, neue Geräte zu kaufen. Der Ärger beschränkt sich nicht auf die Kosten für den Kauf der neuen Geräte. Der Rattenschwanz an Aufwand, Kosten und Risiko bei der Übertragung der bisher genutzten Funktionen auf das neue Gerät zieht nach, und ist oft noch ärgerlicher als das Loch, das der Preis des neuen PC im Portemonnaie schlägt.

Eine wahre Geschichte: Die Abläufe in einer Praxis sind auf das Gesamtkonstrukt aus PC, Kartenleser, Drucker, medizinischer Spezialsoftware und Sicherheitskomponenten für die Kommunikation mit Kassen angewiesen. Ohne dieses Konstrukt gibt es keine Behandlung. Also wird der Service für dieses Gesamtkonstrukt selbsterklärten Profis überlassen. Diese Profis werden für einen Betrag, der weit über die Kosten für einen PC und eine Windows-11-Lizenz hinausgeht, mit dem Ersetzen des bisherigen Windows-10-Geräts durch das neue Gerät beauftragt. Der Service-Mitarbeiter kündigt sein Eintreffen in einem Zeitfenster von mehreren Stunden an, das er auch nicht einhält, arbeitet ein paar Stunden am neuen PC, hinterlässt eine Nachricht und verschwindet. Er hinterlässt die Nachricht: Alles funktioniert.

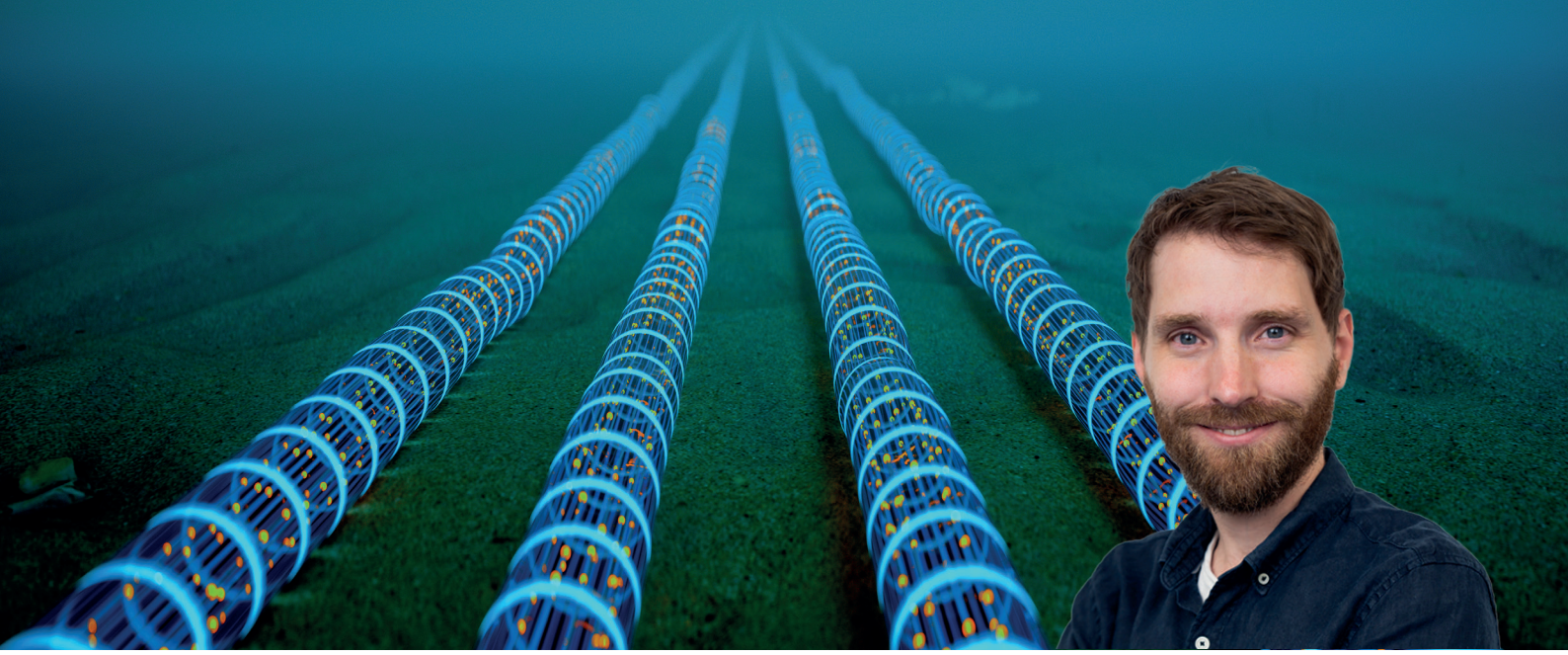
Nichts funktioniert. Das Praxispersonal bekommt nicht einmal das neue Bitlocker-Passwort mitgeteilt. Es folgt minutenlanges Hinterhertelefonieren, um das Passwort zu erfahren. Der PC startet, doch vieles funktioniert nicht: Kein Druckertreiber ist installiert, weder Drucken noch PDF-Versand an andere Einrichtungen ist möglich. Ich erspare Ihnen die Liste fehlender Funktionen. Stundenlanges Hinterhertelefonieren, bis die beauftragte Firma einsieht, dass ein neuer Termin mit dem Service-Techniker erforderlich ist. In der Zwischenzeit müssen viele Patiententermine abgesagt werden. Bis alles wieder funktioniert wie unter Windows 10, vergehen Tage.

## Es mangelt an Kommunikation

Viele wahre Geschichten der oben erzählten Sorte ruinieren den Ruf vom IT-Service allgemein. Ja, die IT ist komplex geworden. Kunden und Dienstleister sind überfordert. Dagegen muss etwas gemacht werden, sonst verbreitet sich die Meinung, das Leben hat sich mit der IT-Durchdringung verschlechtert.

Aus meiner Sicht ist Kommunikation der Schlüssel zur Besserung. Wo Einzelpersonen immer unkommunikativer werden (die Gründe hierfür würden den Rahmen dieses Textes sprengen), ist Kommunikation zu erzwingen.

Der Techniker in unserer wahren Geschichte arbeitet ohne IT Service Management (ITSM). Sein Arbeitgeber (bzw. Auftraggeber, denn häufig gibt es eine ganze Kette von Subunternehmen mit einem Freiberufler als dem letzten Glied) hat kein ITSM oder bindet den Techniker nicht in sein ITSM ein. Mit einem ITSM hätte



# Ein Deep Dive zu den Unterwasser-Datenautobahnen

von Dr. Philipp Rüßmann

Das Leben ohne das Internet ist für uns im Informationszeitalter nicht denkbar. Die Möglichkeit, schnell viele Daten von einem Ende der Welt zum anderen Ende zu übertragen, bestimmt unser alltägliches digitales Leben. Eine besondere Herausforderung stellt dabei die etwa 6.000 km lange Verbindung durch den Atlantik von Europa nach Amerika dar, die wir hier einmal genauer unter die Lupe nehmen wollen. Insbesondere gehen wir dabei auf die Datenübertragung über Glasfasern ein.

Eine kurze Geschichte der transatlantischen Datenübertragungen
Der erste Meilenstein der transatlantischen Datenübertragung wurde bereits 1858 gelegt [1]. Es dauerte vier Jahre, bis das erste Telegramm durch ein Unterseekabel, das die Verbindung von Irland nach Neufundland durch den Atlantik herstellte, von Queen Victoria an Präsident James Buchanan gesendet werden konnte. Allerdings war diese Verbindung weder schnell noch stabil. Das Senden der 98 Wörter vom Vereinigten Königreich nach Amerika dauerte 67 Minuten, aber es brauchte ganze 16 Stunden, bis die Bestätigungskopie der Übertragung wieder in Irland ankam.

Innerhalb sehr kurzer Zeit ging die Signalqualität weiter rapide in den Keller. Uneinigkeiten über die Art des Endgerätes führten dazu, dass auf jeder Seite unterschiedliche Gerätschaften zum Einsatz kamen. Bei mehreren Versuchen, durch höhere Spannungen von bis zu 2.000 V ein schnelleres Signal zu übermitteln, wurde die Isolierung des Kupferkabels stark beschädigt. Das Kabel der Atlantic Telegraph Company war nach nur drei Wochen im Betrieb zerstört. Wie heute solche Kabelschäden lokalisiert und repariert werden, hat mein Kollege Dr. Joachim Wetzlar in einem Artikel des Netzwerk Insiders beschrieben.

Seit diesen ersten Versuchen hat sich jedoch viel getan. Statt isolierter Kupferkabel ist seit den späten 80er Jahren die Übertragung per Glasfaser das Mittel der Wahl. Wie in Abbildung 1 gezeigt, verfügt ein modernes Kabel über eine gewisse Zahl an Lichtwellenleitern (LWL), die durch mehrere Schichten aus Plastik und Metallhüllen vor äußeren Einflüssen geschützt werden.

Dieses Prinzip lässt sich auch gut skalieren; je mehr LWL im Kern des Kabels verstaut werden, desto höher kann auch die Bitrate ausfallen. So erreicht z.B. das im September 2022 von Google

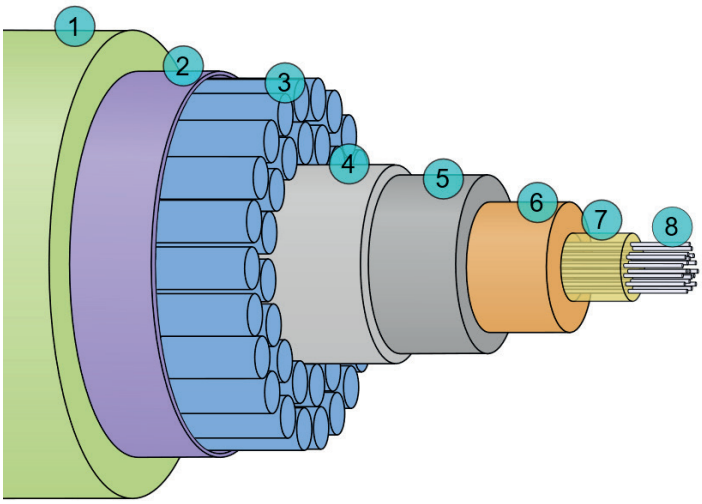



Abbildung 1: Typischer Querschnitt eines modernen Unterseekabels. Von außen nach innen: 1 – Polyethylene, 2 – Polyester-Band, 3 – Stahldrähte, 4 – Aluminium-Wasserschutz, 5 – Polycarbonat, 6 – Kupfer- oder Aluminiumrohr, 7 – Vaseline, 8 – Lichtwellenleiter. Quelle: Oona Räisänen [2].

# Prüfung von Ladekabeln für Elektroautos

von Peter Steufmehl

Das Ladekabel für Elektrofahrzeuge (EV, Electric Vehicle) ist mehr als ein einfacher Stromleiter. Es handelt sich um eine hochentwickelte, sicherheitsrelevante Systemkomponente, die eine kontinuierliche bidirektionale Kommunikation der Ladestation mit dem Elektrofahrzeug aufrechterhält, um den Ladevorgang präzise zu steuern und zu überwachen. Eine Fehlfunktion in dieser kritischen Verbindung kann nicht nur den Ladevorgang verhindern, sondern auch zu schwerwiegenden Schäden am Fahrzeug oder der Ladeinfrastruktur führen und im schlimmsten Fall lebensgefährliche Situationen wie Brände oder Stromschläge verursachen. Dieser Blog liefert eine systematische Anleitung, wie die Integrität dieser entscheidenden Komponente überprüft werden kann, mit einer klaren Abgrenzung zwischen den Prüfschritten für technisch versierte Laien und den normativ vorgeschriebenen, tiefgehenden Prüfungen für qualifizierte Fachkräfte.

## Sicherheit und Zuverlässigkeit von EV-Ladekabeln

Die Relevanz einer solchen systematischen Prüfung wird durch statistische Daten untermauert. Eine Studie des Bundesamts für Wirtschaft und Ausfuhrkontrolle (BAFA) aus dem Jahr 2020 zeigt, dass von den insgesamt 2500 durchgeführten UVV-Prüfungen (UVV: Unfallverhütungsvorschrift) an Ladekabeln für Elektrofahrzeuge 15 % aufgrund von Mängeln aus dem Verkehr gezogen oder zwingend zu reparieren waren. Diese überraschend hohe Fehlerquote belegt, dass die potenziellen Gefahren durch defekte Ladekabel real sind, und unterstreicht die Notwendigkeit einer regelmäßigen Überprüfung, die über eine rein optische Inspektion hinausgeht. Für Arbeitgeber und Betreiber von E-Fahrzeugflotten hat dies erhebliche Auswirkungen.

Die Wartung und wiederkehrende Prüfung von Ladekabeln ist keine optionale Vorsichtsmaßnahme, sondern eine gesetzliche Verpflichtung gemäß der DGUV-Vorschrift 3 (ehemals BGV A3), die die Sicherheit am Arbeitsplatz gewährleisten soll. Eine Vernachlässigung dieser Pflicht kann zu rechtlichen Konsequenzen führen. Aus diesem Grund ist eine umfassende Betrachtung der Thematik unerlässlich, die nicht nur die technischen Aspekte der Prüfung, sondern auch die zugrunde liegenden Sicherheits- und Rechtsnormen beleuchtet.

## Aufbau eines Ladekabels und die Rolle der Kommunikation

Das Herzstück der modernen Ladeinfrastruktur in Europa ist der Typ-2-Stecker, der sich durch eine flexible Anwendbarkeit im ein- bis dreiphasigen Betrieb auszeichnet und eine sichere, signalgesteuerte Verriegelung bietet. Die Funktionalität des Kabels basiert auf einem komplexen System aus insgesamt sieben Kontaktstiften, die in zwei Hauptgruppen unterteilt sind.

Die erste Gruppe umfasst fünf Hauptleiter, die für die eigentliche Energieübertragung zuständig sind:

- Drei Außenleiter (L1, L2, L3): Diese sind für die Übertragung von Wechselstrom im dreiphasigen Netz verantwortlich.
- Ein Neutralleiter (N): Dieser dient als Rückleiter für den Stromkreis.
- Ein Schutzleiter (PE): Der Schutzleiter ist die wichtigste Sicherheitsader. Er leitet im Fehlerfall gefährliche Fehlströme sicher ab und dient als Referenzpunkt für die Niederspannungssignale, die über die Kommunikationsadern übertragen werden.

# Handover zwischen WLAN-Call und VoLTE in der Praxis

Mit Sara Mohd Shafek sprach Christiane Zweipfennig

Wireless Local Area Network (WLAN) ist heute nahezu überall verfügbar, wodurch der Internetzugang unabhängig von der Mobilfunkverbindung möglich wird. WLAN-Call ermöglicht, Telefonate über die eigene Mobilfunknummer auch ohne Verbindung mit dem öffentlichen Mobilfunknetz durchzuführen. Ein zentraler Aspekt von WLAN-Call ist die Fähigkeit des Endgeräts, automatisch und ortsunabhängig zwischen Netzen zu wechseln, ohne dass der Nutzer während dieser Übergabe Service-Einschränkungen erlebt. Dieser Vorgang der Verbindungsübergabe wird als Handover bezeichnet. Ziel ist es, eine nahtlose, unterbrechungsfreie Kommunikation zwischen WLAN und öffentlichem Mobilfunknetz sicherzustellen.

Sara Mohd Shafek ist im Jahr 2021 bei ComConsult als studentische Hilfskraft eingestiegen. Nach einem Orientierungssemester im Fach Elektrotechnik entschied sie sich für ein Bachelorstudium an der FH Aachen. Im Rahmen ihres Studiums absolvierte sie ein sechswöchiges Berufspraktikum bei ComConsult, in dessen Verlauf sie sich mit dem Thema WLAN-Call – auch als WiFi Calling bezeichnet - beschäftigte und dazu eine Reihe von Tests durchführte. Dadurch eignete sie sich die Grundlagen an und entschloss sich, das Thema in ihrer Bachelorarbeit, die ebenfalls von ComConsult betreut wurde, sowohl theoretisch als auch praktisch vertieft zu bearbeiten.

## Was war die Motivation deiner Bachelorarbeit?

Die Motivation für diese Bachelorarbeit ergab sich aus der zunehmenden Bedeutung von WLAN-Call in Unternehmen und den damit verbundenen Herausforderungen der Mobilfunkversorgung. Smartphones sind mittlerweile unverzichtbar, um zeitlich und örtlich unabhängig kommunizieren zu können. Gleichzeitig reicht die Abdeckung öffentlicher Mobilfunknetze nicht überall aus: Zum einen betrifft dies ländliche Gebiete, doch auch in vielen Städten beeinträchtigen Fassadendämpfungen und großflächige Fensterverglasungen neuer Gebäude die Signalqualität von Mobilfunk. Während meiner Zeit als studentische Hilfskraft war ich an den Mobilfunkmessungen bei einem Kunden beteiligt. Bei dem Konzern war die Mobilfunkversorgung in einigen Bauten auf dem Campus extrem schwach, und die Mitarbeiter beschwerten sich wiederholt über den unzureichenden Empfang.

Die Ausstattung von Wireless Local Area Networks (WLAN) wird in der heutigen Zeit nahezu überall vorausgesetzt. Dadurch lässt sich der Internetzugang eines Nutzers unabhängig vom Mobilfunknetz herstellen. WLAN-Call ist darauf ausgelegt, Telefongespräche auch ohne Verbindung zum öffentlichen Mobilfunknetz zu ermöglichen.

WLAN-Call erlaubt dem Endgerät, automatisch zwischen Netzen zu wechseln – unabhängig von den räumlichen Gegebenheiten – ohne Einschränkungen für den Nutzer. Dieser Vor-

> Handover zwischen WLAN und öffentlichem Mobilfunknetz muss für eine unterbrechungsfreie Kommunikation nahtlos funktionieren.

# Supply-Chain-Angriffe und ihre Auswirkungen

von Dr. Markus Ermes

Und wieder macht ein neuer erfolgreicher Cyberangriff Schlagzeilen: Unter Titeln wie „BER nach Cyberangriff lahmgelegt“ wurde in den letzten Wochen darüber berichtet, dass ein Angriff verschiedene Flughäfen in Deutschland lahmgelegt oder zumindest den Check-in für die Passagiere deutlich zeitaufwendiger gemacht hat. Was ist passiert? Zäumen wir das Pferd von hinten auf!

## Auswirkungen

Verschiedene Flughäfen in Deutschland hatten über längere Zeit deutliche Probleme mit ihrem Check-in – in manchen Fällen war er so gut wie unmöglich, in anderen Fällen musste auf analoge Verfahren umgestellt werden, was zu erheblichen Verzögerungen geführt hat. Und hier ist schon der erste indirekte Hinweis auf die Ursache: Analoge Prozesse funktionierten, also ist irgendetwas Digitales schiefgegangen. Doch dazu später mehr.

Was besonders auffiel: Wer nur den Titel der Schlagzeile gelesen hatte und dachte: „Schon wieder ein erfolgreicher Angriff auf die Infrastruktur! Die vom BER scheinen es auch nicht wirklich draufzuhaben,“ bekam einen vollkommen falschen Eindruck. Betroffen waren nämlich nicht nur der Flughafen BER, auch wenn dieser aufgrund seiner Geschichte vielleicht der bekannteste unter den beeinträchtigten Flughäfen war.

Hinzukam, dass zwar einige der größeren Flughäfen betroffen waren, aber längst nicht alle und auch nicht im gleichen Ausmaß. Doch wenn es ein Angriff auf BER gewesen sein sollte, wie konnte er sich dann auf andere Flughäfen auswirken?

Und hier liegt mein größter Kritikpunkt an vielen der Schlagzeilen: Um Aufmerksamkeit zu generieren, wurden die Tatsachen für den Titel sehr verkürzt und – wahrscheinlich bewusst – ungenau dargestellt. Denn die Ursache war eben nicht, dass der Flughafen BER angegriffen wurde.

Aber was steckte dann dahinter?

## Die eigentliche Ursache

Die Ursache, die auch erklärt, warum mehrere Flughäfen betroffen waren, lag woanders: Ein bei vielen Flughäfen für den Check-in beauftragter Dienstleister wurde erfolgreich angegriffen. Die Flughäfen haben daraufhin ihre Netzwerk-Verbindungen zu diesem Dienstleister so schnell wie möglich gekappt, um nicht selbst Ziel eines (weiteren) Angriffs zu werden. Also war es nicht die Schuld eines oder mehrerer Flughäfen, sondern es handelte sich um einen klassischen Supply-Chain-Angriff, in dem ein Glied der Lieferkette kompromittiert wird und damit andere Glieder der Kette ebenfalls betroffen sein können. In vielen Fällen dient die Kompromittierung eines Dienstleisters oder Lieferanten dazu, die Belieferten anzugreifen. Hier war jedoch reine Sabotage das Ziel. Dass der Flughafen BER zwei Wochen gebraucht hat, bis das Problem behoben wurde (ebenfalls beim Dienstleister), zeigt, dass die Sabotage recht erfolgreich war.

Leider nehmen diese Angriffe zu, sodass man sich auch selbst die Frage stellen muss: Was passiert, wenn es einen meiner Zulieferer erwischt oder ich als Zulieferer eines anderen Unternehmens ins Visier gerate?