



Liebe Leserin,  
lieber Leser

Können Sie sich noch an die Panzerknacker erinnern? Die drei stoppelbärtigen Bösewichte aus Entenhausen? Was in den Geschichten von damals als dreistes Verbrechen galt, mag uns heute nur noch ein nostalgisches Lächeln entlocken.

In der heutigen Zeit werden wir mit anderen Delikten konfrontiert: Lesen Sie das Editorial zum Thema Cyberkriminalität meines Geschäftsleitungskollegen Fabio Alberini und den entsprechenden Artikel auf Seite 2 in diesen News. Da gehts ums Knacken von Daten, Systemen, Passwörtern. Und um weitaus grösseren Schaden als denjenigen, den Dagebert Duck von der Panzerknackerbande befürchten musste.

Auch wir von Fraumünster sind Spezialisten im Knacken. Nicht von Geldspeichern oder Daten. Wir sind Profis im Problemerkacken. Mit viel Biss und Ausdauer geben wir nicht auf, bis wir die perfekte Lösung haben. Bleiben dran, bis ein Resultat vorliegt, das auf Ihre Ansprüche massgeschneidert ist. Nicht selten entstehen so Versicherungsprodukte, die den Markt nachhaltig verändern.

Wir sind seit vielen Jahren Ihre Versicherungsprobleme-Knacker. Was uns von den legendären drei Panzerknackern unterscheidet: Wir stellen uns geschickter an. Und sind wesentlich besser rasiert!

IHR MARCO SCHLATTER



Liebe Kundin,  
lieber Kunde

Ist die Digitalisierung Fluch oder Segen? Unbestritten ist, dass sie uns viele Vorteile bringt: vereinfachte und schnellere Prozesse, Kostenoptimierung, Übersichtlichkeit. Leider hat wie alles im Leben, auch diese Medaille zwei Seiten ...

Diese immense Datenmenge muss aufbewahrt werden. Dabei stellen sich Fragen wie: Was muss, soll und darf überhaupt gespeichert werden? Wer ist dafür verantwortlich? Welche Daten sind sensibel und ganz besonders schützenswert? Nicht immer sind die Antworten darauf klar.

Schwierig und gefährlich wirds, wenn sich Hacker gezielt Zugang zu diesen Informationen und Dokumenten verschaffen. Internetkriminalität ist eine Gefahr, vor der niemand gefeit ist, und die uns in Zukunft zunehmend beschäftigen wird. Technische Sicherheiten sind dabei das eine, die entsprechende Versicherungslösung das andere.

Wir haben für Sie das Wichtigste zu Datenschutz und Versicherungsprodukte zu Cyberattacken und -crime zusammengetragen. Sie lesen den Artikel auf Seite 2 dieser News.

Ich wünsche Ihnen einen schönen Sommer - und dass Sie ihn möglichst analog geniessen können.

IHR FABIO ALBERINI

## Fraumünster- Apéro

Wie, wann und wo? Das ist noch unser kleines Geheimnis. Aber so viel sei verraten: Dieses Jahr wird alles anders. Was aber bleibt: die Freude, mit Ihnen zusammen zu sein und bei Häppchen und einem feinen Tropfen gemeinsame Zeit zu verbringen.

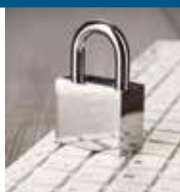
Die Einladung mit näheren Infos folgt. Wir freuen uns jetzt schon auf Sie!



UNTER ANDEREM IN DIESER AUSGABE



**Cyberattacken und  
-crime - eine echte  
Bedrohung?**



**Neue EU-Datenschutz-  
Grundverordnung**



**Was kommt nach  
der Vollversicherung?**

# Cyberattacken und -crime – eine echte Bedrohung?

Die Medien berichten regelmässig von Cyberattacken oder Diebstählen von Geldern mithilfe von digitalen Mitteln. Sind das für Sie nur Schlagwörter, oder machen Sie sich auch Gedanken dazu? Gemäss vieler Studien werden diese Bedrohungen als gross wahrgenommen. Trotzdem, der Anteil der Unternehmen, die das Risiko der Folgen einer Cyberattacke oder einer Veruntreuung (Cybercrime) mittels Versicherung überwältigt haben, ist noch gering. Die Argumente gehen von «wir sind doch kein interessantes Ziel» über «unsere Daten sind im Rechenzentrum» bis zu «nein, auf Geldüberweisungen kann niemand Einfluss nehmen, die sind sicher». Wenn dem so wäre, warum passieren immer wieder Attacken und Diebstähle? Trifft es immer nur Unternehmen, die nicht in die Sicherheit investiert haben? Bestimmt nicht. Die Opfer der Attacken sind – zumindest diejenigen, von denen man erfährt – immer grosse Firmen mit entsprechenden Budgets für IT und Sicherheit. Wie schwierig wird es wohl sein, Ihr System zu hacken? Oftmals genügt ein gut platzierter USB-Stick mit einer ansprechenden Beschriftung wie «Löhne» oder «Bewerbung»

vielleicht auch «Projekt XY». Hauptsache, etwas, das die Neugier weckt. Mit Sicherheit möchte jemand den Inhalt des Memory-Sticks lesen und wird diesen im Gerät einstecken. Bloss ist der Inhalt nicht wie angeschrieben, sondern eine Schadsoftware, die einem unbefugten Dritten Zugang zu Ihrem System gewährt und diesen nun schalten und walten lässt und Sie selbst ausschliesst.

Was nun? Einfach das Gerät vom Netz nehmen und hoffen, dass keine weitere Verbreitung stattgefunden hat? Der erste Punkt ist sicher in den meisten Fällen nicht fehl am Platz. Jedoch ist es damit selten getan. Nun kommt das Ganze nämlich erst so richtig ins Rollen. Oftmals ist ein Virus so programmiert, dass er umgehend die Netzwerkumgebung infiziert und sich «durchfrisst». Auf jeden Fall wird die IT-Abteilung oder der externe Support sofort kontaktiert, um hoffentlich allem ein Ende zu setzen. Ist diese Stelle fit für eine Cyberattacke mit grosser Auswirkung? Wissen diese Leute genau, was zu tun ist und wer allenfalls benachrichtigt werden muss? Was, wenn der Virus über das eigene Netz bereits an Dritte übertragen wurde? Es ist ratsam,

bei einer Cyberattacke ein Krisenmanagement zur Hand zu haben. Dieses unterstützt die internen Stellen mit einer externen Expertise und den notwendigen Fachkräften. Dies können Forensiker, PR-Spezialisten, Anwälte, Betrugsspezialisten und selbstverständlich IT-Spezialisten etc. sein. Bis zu diesem Punkt sind die Folgen des Vorfalls noch nicht behoben, nur der Pfad wird festgelegt. Alleine so ein Spezialisten-Team wird sicher seinen Preis haben. Dann folgen die Kosten für die Behebung des Vorfalls (z. B. Entfernen eines Crypto-Lockers, Wiederherstellen von gelöschten oder veränderten Daten, Behebung eines Betriebsunterbruchs, Notifizierung von Dritten, Verletzung von geistigem Eigentum etc.). Zudem ist per 25. Mai 2018 die neue Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO) in Kraft getreten. Diese hat auch auf Unternehmen in der Schweiz Einfluss. Dies, sobald Kundenbeziehungen in die EU oder Niederlassungen in der EU bestehen. Abgesehen von Kosten zur Wiedererlangung des Zustands vor der Attacke können als Folge einer Cyberattacke oder des Zugriffs durch einen Hacker auch Zahlungsdaten verändert oder falsche Kontoverbindungen zu bestehenden Kunden oder Lieferanten übermittelt oder kommuniziert werden. In diesen Fällen spricht man von «Social Engineering Fraud». Dies ist heute leider sehr stark verbreitet: Der Versuch dazu ist bei fast jedem Unternehmen in einer der vielen Formen vorgekommen. Oftmals ist es leider nicht nur beim Versuch geblieben, sondern Gelder wurden tatsächlich an falsche Konten überwiesen oder Zahlungsanweisungen wurden in den internen Systemen vor der Übermittlung an die Bank so verändert, dass auch diese an andere Empfänger umgeleitet wurden. In diesen Fällen haftet nicht das Zahlungsinstitut für Ihren Verlust, sondern einzig Sie selbst.

Cyberattacken und -crime betreffen leider alle, man kann sich diesen Themen nicht verschliessen. Wir erläutern wichtige Fragen und helfen Ihnen, Lösungen zu finden, die die beschriebenen Szenarien kalkulierbar machen. Melden Sie sich!

**PHILIPP SPIEGEL**

Mandatsleiter

D +41 44 444 29 18

[philipp.spiegel@fraumuenster.com](mailto:philipp.spiegel@fraumuenster.com)





## Was kommt nach der Vollversicherung?

Am 10. April 2018 hat AXA als zweitgrösster privater Anbieter der BVG-Vollversicherungen in der Schweiz mitgeteilt, dass sie ab 1. Januar 2019 keine Vollversicherungen mehr anbietet. Die betroffenen Kunden werden in eine teilautonome Sammelstiftung transferiert und erhalten für den Fall, dass sie nicht einverstanden sind, ein Kündigungsrecht bis zum 30. November 2018.

Was in der Branche schon länger vermutet wurde, ist nun Tatsache geworden. AXA hat wahrscheinlich eine Vorreiterrolle eingenommen. Bereits im 2004 war sie (damals noch Winterthur) die erste Lebensversicherungsgesellschaft, die das sogenannte Splitting-Modell eingeführt hatte (unterschiedliche Zins- und Umwandlungssätze im Obligatorium und Überobligatorium). Man spricht heute noch vom «Winterthur-Modell».

### Vollversicherungen, quo vadis?

Schon seit einiger Zeit stellen wir fest, dass die privaten Lebensversicherer ihre teilautonomen Produkte vermehrt pushen. Gleichzeitig fahren sie in der Vollversicherung eine immer restriktivere Annahmepolitik. Der Schutz des Versichertenbestandes ist eine zentrale Aufgabe jedes Anbieters der beruflichen Vorsorge. So haben kleine KMU mit gesetzesnahen Leistungen, geringen überobligatorischen Altersguthaben, ungünstiger Altersstruktur (Mitarbeitende ab Alter 55) oder höherem Schadenrendement grosse Mühe, eine Vollversicherung zu finden. Vollversicherung bedeutet, dass nebst den Risiken Tod und Invalidität auch das Anlagerisiko übernommen wird, oder anders gesagt, es besteht eine Kapitalerhaltungs- und Zinsgarantie, unabhängig der Finanzmarktlage. Garan-

tien sind für die Kunde nicht gratis. Diese Sicherheit schlägt sich in der Risikokostenprämie nieder. Aufgrund dieser Garantiever-sprechungen können die Vollversicherungsanbieter das Vorsorgevermögen nicht gross in volatile Anlageklassen investieren, da sie jederzeit ihren finanziellen Verpflichtungen nachkommen müssen. Reguliert werden sie durch die Finma und sie unterstehen den harten Auflagen des Swiss Solvency Tests, während in der teilautonomen Welt die kantonalen Aufsichtsbehörden zuständig sind. Wegen des kleinen Handlungsspielraums der Lebensversicherer, den ungünstigen Rahmenbedingungen und der finanziellen Lage – geprägt vom hartnäckig anhaltend tiefen Zinsniveau sowie der demografischen Entwicklung –, erwarten wir weitere Veränderungen in der Vollversicherung. Ob aus fünf Anbietern noch weniger werden, ist schwierig abzuschätzen. Es bestehen noch andere Möglichkeiten oder Massnahmen, wie Wegfall des gesplitteten Umwandlungssatzes oder zwingende Erhöhung der Altersgutschriften, mit denen in der Zukunft zu rechnen ist. Zurzeit haben sich alle fünf verbliebenen Anbieter eindeutig zur Vollversicherung bekannt. Klar ist, dass die Nachfrage der KMU nach diesem Produkt grösser ist als das Angebot. Viele KMU wünschen sich Sicherheit und nehmen die höheren

Kosten in Kauf, da sie das Anlagerisiko nicht tragen wollen oder können.

### Beide Produkte haben ihre Existenzberechtigung

Welches Produkt für welches KMU geeignet ist, hängt unter anderem von Risikowilligkeit und Risikofähigkeit des Unternehmens ab. Ein Unternehmen mit vielen jungen Angestellten weist beispielsweise einen längeren Anlagehorizont auf und kann den Fokus eher auf höhere Renditeerwartungen legen.

### Teilautonome Sammelstiftungen

Um bei den teilautonomen Stiftungen den passenden Anbieter zu finden, gibt es nebst den reglementarischen Bestimmungen eine Vielzahl an technischen Parametern zu beachten.

Kommen Sie auf uns zu – wir unterstützen Sie gerne mit unserem fundierten Fachwissen bei der Auswahl des auf Ihre Bedürfnisse und Wünsche zugeschnittenen BVG-Anbieters und begleiten Sie auch gerne über einen allfälligen Wechsel hinaus.

### AURELIA HEMMELER

Mitglied der Geschäftsleitung

D +41 44 444 29 07

aurelia.hemmeler@fraumuenster.com

# Fraumünster präsentiert: TIXI Zürich

## Mobil sein macht selbstständig

Ein Theaterbesuch, die Fahrt ins tägliche Training oder der Weg zum Stammtisch – kein Problem? Für mobilitätsbehinderte Menschen kann die Teilnahme am gesellschaftlichen Leben eine grosse Herausforderung sein. Hier kommt TIXI Zürich ins Spiel.

«Ich freue mich jedes Mal,  
wenn das TIXI-Auto vorfährt.»

(Thomas Merten, TIXI-Fahrgast)

Der gemeinnützige Verein hat das Ziel, die Mobilität von Menschen mit Behinderung und von Betagten zu erhalten. Mit den speziell für diese Aufgabe umgebauten Fahrzeugen wird der Gast am gewünschten Ort abgeholt und sicher zum Wunschort gebracht. Geleistet wird diese Aufgabe durch aktuell 400 ehrenamtlich tätige Fahrerinnen und Fahrer. Sie werden oft schon erwartet und freudig begrüsst. Manchmal kennt man sich bereits und tauscht sich aus. Die Fahrer helfen beim Ein- und Aussteigen und kümmern sich um die Fahrgastsicherheit. 1,4 Millionen Fahrkilometer legen sie jedes Jahr zurück,

um den Besuch bei der Familie zum gemeinsamen Zmittag oder ein unvergessliches Konzerterlebnis zu ermöglichen.

Gefahren wird von morgens von 7.30 Uhr bis nachts um 23.30 Uhr – an Wochenenden und Feiertagen ab 9.30 Uhr. In der Zentrale stehen dafür 23 Mitarbeitende im Einsatz. Sie betreuen und schulen die 400 ehrenamtlichen Fahrerinnen und Fahrer, sorgen für die reibungslose Planung der mehr als 5000 Fahrten monatlich und den notwendigen Fuhrpark. Die finanziellen Mittel, um zu konkurrenzlos günstigen Tarifen ein Stück Lebensqualität für mobilitätseingeschränkte Menschen anbieten zu können, stammen zu 60 Prozent von privaten Spendern und Sponsoren. Zusätzlich zum Fahrpreis, der vom Fahrgast entrichtet wird, muss TIXI für jede Fahrt rund 40 Franken Spendengelder einbringen.

**Jede Spende sichert ein Stück  
Freiheit und Autonomie!**

**Konto 80-14900-0 Postfinance  
IBAN CH04 0900 0000 8001 4900 0  
SWIFT POFICHB**

TIXI Zürich ist ein gemeinnütziger Verein, der mobilitätsbehinderten Menschen helfen will, sich selbstbestimmt fortzubewegen und so am sozialen Leben teilzunehmen. Neben der gesellschaftlichen Integration steht die Gleichstellung behinderter Menschen im öffentlichen Raum im Zentrum.

Der Fahrdienst ermöglicht Menschen, die die öffentlichen Verkehrsmittel nicht ohne Hilfe nutzen können, selbstbestimmte Mobilität. Dies erleichtert es ihnen, soziale Kontakte zu pflegen und ihren Alltag abwechslungsreich zu gestalten.

Der Verein strebt keinen Gewinn an. Alle Fahrer und Fahrerinnen leisten ihren Dienst in Freiwilligenarbeit. Der Vorstand arbeitet ehrenamtlich.



**TIXI Zürich**

Fahrdienst für Menschen  
mit Behinderung  
Mühlezelgstrasse 15  
CH-8047 Zürich  
Tel. +41 44 404 13 80  
www.tixi.ch



# Neue EU-Datenschutz-Grundverordnung

Seit 25. Mai 2018 ist die neue EU-Datenschutz-Grundverordnung (DSGVO) anwendbar, die das Ziel hat, das Datenschutzrecht innerhalb Europas zu vereinheitlichen sowie den Datenschutz den neusten technologischen Entwicklungen anzupassen.

Die erhöhten Anforderungen und Pflichten sind umfassend und haben auch Einfluss auf Schweizer Unternehmen. Beispielsweise, wenn diese Waren und Dienstleistungen Personen mit Wohnsitz in der EU anbieten und dabei deren Daten bearbeiten oder in der Schweiz für Unternehmen in der EU Rechenzentren betreiben. Für Unternehmen, die Tochtergesellschaften oder Niederlassungen im EU-Raum besitzen, gilt die DSGVO auch dann, wenn die Daten in der Schweiz bearbeitet werden.

Auch schweizerische Unternehmen wie zum Beispiel Hotels oder Online-Shops sind davon betroffen, wenn via Website oder per App Angebote an Personen in der EU gemacht werden und dabei Personendaten von Personen mit Wohnsitz in der EU gesammelt werden oder das Verhalten von diesen Personen analysiert wird.

Nicht betroffen sind beispielsweise Unternehmen, die Personendaten von Personen mit Wohnsitz in der Schweiz oder ausserhalb der EU in der Schweiz oder ausserhalb der EU bearbeiten. Es ist aber zu beachten, dass das Schweizerische Datenschutzgesetz (DSG) in naher Zukunft revidiert und dem EU-Datenschutzrecht angepasst wird.

Das Gesetz gilt ebenfalls nicht für Daten, die sich auf juristische Personen beziehen, oder für Tätigkeiten im Rahmen von familiären und privaten Bereichen.

Mit der DSGVO werden die personenbezogenen Daten von natürlichen Personen geschützt bzw. alle Informationen, die die Identifizierung einer natürlichen Person ermöglichen.

In der DSGVO sind unter anderem folgende Pflichten geregelt:

- Der Schutz der Daten muss durch organisatorische und technische Massnahmen unter Berücksichtigung des Standes der Technik jederzeit gewährleistet sein. Zum Beispiel müssen datenschutzfreundliche



Voreinstellungen sicherstellen, dass die Daten nicht zweckentfremdet werden. Zudem ist fallbezogen eine Anonymisierung und Verschlüsselung personenbezogener Daten sicherzustellen.

- Die Einwilligung der Betroffenen muss eindeutig sein und diese kann jederzeit widerrufen werden. Eine stillschweigende Zustimmung genügt nicht mehr. Diese muss mittels einer klaren Einwilligungserklärung erfolgen. Ebenfalls bestehen ausführliche Informationspflichten, aufgrund derer die Betroffenen darauf aufmerksam gemacht werden, wie und zu welchem Zweck die Daten bearbeitet werden.
- Es bestehen umfassende Regeln zur Pflicht der Datenschutz-Folgeabschätzung (Risikoanalyse) und Dokumentationspflichten der eigenen Prozesse zur Verarbeitung von Daten, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben.
- Für datenverarbeitende Unternehmen besteht die Pflicht, einen Vertreter mit Sitz in der EU zu ernennen, sofern keine Niederlassung in der EU besteht. Von dieser Pflicht ausgeschlossen sind Firmen, die nur gelegentlich und keine umfassenden Datenverarbeitungen vornehmen.
- Datensicherheitsverstösse bezüglich personenbezogenen Daten mit Auswirkung auf die Betroffenen (z.B. bei Identitätsdiebstahl) sind den entsprechenden Datenschutzbehörden innert 72 Stunden zu melden. Ebenfalls ist eine unverzügliche Benachrichtigung an die Betroffenen notwendig, wenn ein hohes Risiko im Zusammenhang mit den persönlichen Rechten und Freiheiten besteht.

Es gilt das Prinzip der Beweislastumkehr. Das heisst, bei einem Verstoss muss das betroffene Unternehmen belegen, dass sämtliche Datenschutzregeln eingehalten wurden. Bei Verletzung der Vorschriften drohen Bussen bis zu 20 Mio. Euro oder 4 Prozent des weltweiten Jahresumsatzes – je nachdem, welcher Betrag höher ist.

## Versicherungsmöglichkeiten

Eine umfassende Cyberversicherung deckt unter anderem einen Vermögensschaden Dritter im Zusammenhang mit Datenschutzverletzungen ab. Ebenfalls enthalten sind die Abwehrkosten bei behördlichen Verfahren (inkl. Verteidigungs- und Verfahrenskosten), Strafen und zivilrechtliche Bussen (sofern gemäss anwendbarem Recht versicherbar) sowie Abwehr- und Mehrkosten.

Nehmen Sie mit uns Kontakt auf, wir helfen Ihnen gerne weiter!

## PHILIPP FORSTER

Mitglied der Geschäftsleitung  
D +41 44 444 29 13  
philipp.forster@fraumuenster.com

## NEWS

### Welche Fragen haben Sie?

Liebe Leserinnen und Leser  
Welche Themen interessieren Sie?  
Worüber möchten Sie detaillierter informiert werden? Welche Fragen haben Sie? Wir freuen uns auf Ihr Feedback auf [news@fraumuenster.com](mailto:news@fraumuenster.com). Vielleicht ist Ihr Input schon bald Thema in den nächsten News.

# Fraumünster-Jubilarin und -Jubilare



**Wolfgang Mittelmeyer**  
(15 Jahre)



**Elena Bachmann**  
(5 Jahre)



**José Maria Fraile**  
(5 Jahre)



**Pascal Merlo**  
(5 Jahre)

<b>Das bin ich:</b>	Interessiert und geduldig	(Fast) immer vor 8 Uhr im Büro	Selten vor 8 Uhr im Büro	Chef des organisierten Chaos auf meinem Schreibtisch
<b>Dieses Lied läuft auf meinem iPod rauf und runter:</b>	«You and your friend» von Dire Straits	«Havana» von Camila Cabello	«Sweet Coffee» von Mullally feat. Bassette, aber auf dem iPhone	«Photosynthesis» von Frank Turner
<b>Dafür würde ich mitten in der Nacht aufstehen:</b>	Für Sternschnuppen	Für eine Reise nach Hawaii	Für Läderach-Schoggi, 48h Sale Swiss	Für die selbstgemachten Hamburger meiner Mutter
<b>Dafür bin ich dankbar:</b>	Gesundheit	Mit Seelenverwandtem José Fraile zu arbeiten	Mit Seelenverwandten Elena Bachmann zu arbeiten	Eldorado Craft Beer Bar in Zürich
<b>Mit dieser Person würde ich gerne einmal lunchen:</b>	Laurie Anderson	Channing Tatum	Deadpool, ohne Maske	Marilyn Manson
<b>Von diesem Wunsch weiss noch niemand:</b>	Das soll auch so bleiben!	Siehe vorherige Frage ...	Wünsche darf man nicht verraten ...	Habe ich gerade wieder vergessen ...
<b>Deshalb bin ich bei der Fraumünster:</b>	Interessante Arbeit und gutes Arbeitsklima	Beste Znüni-Verpflegung durch die Arbeitskollegen	Ich mag Familienschläuche. Wirklich!	Wegen der hohen Fachkompetenz, der ausgeprägten Znüni-Kultur und den Glaces im Kühlschrank!

## UNSERE PARTNERFIRMEN



### Fraumünster Insurance Experts

Scheffelstrasse 12  
Postfach, CH-8042 Zürich  
Tel. +41 44 444 29 00  
Fax +41 44 444 29 01

Büro Basel  
Aeschenplatz 4  
CH-4052 Basel  
Tel. +41 61 201 20 00  
Fax +41 61 201 20 01

info@fraumuenster.com  
www.fraumuenster.com