Gefahren, Auswirkungen,

Unterstützung:

Die CYBERVERSICHERUNG

Überblick

- Cyber: Aktueller Status Quo
  - Kriminalität, Fallbeispiel, Gefahren
- Verständnis und Strukturen des Cyberkrisenmanagements
- Arten von Cyber-Bedrohungen
- Cyber-Auswirkungen
- Wie kann Unterstützung gegeben werden: Die Cyber-Versicherung

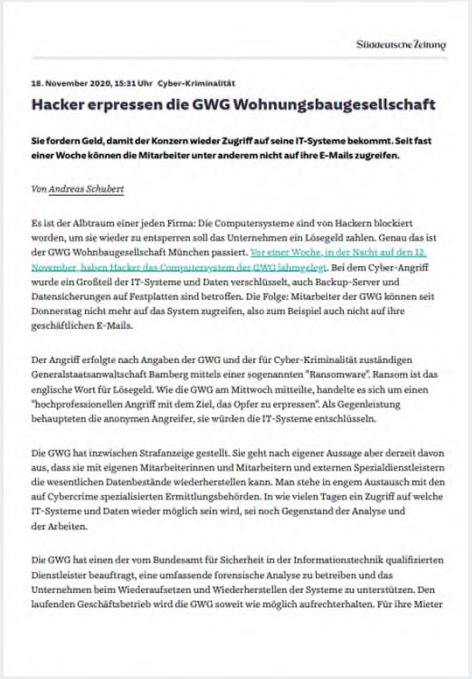
Cyber: Aktueller Status Quo

Kriminalität - Ein reales Risiko für Wohnungsunternehmen

- Cyber-Kriminalität wird immer noch oft unterschätzt, dabei ist es inzwischen ein alltägliches Phänomen
- Jeder Betrieb verfügt über Daten, die für Hacker von hohem Interesse sind: Kontodaten und Kreditkartendaten, Gesundheitsdaten, Personaldaten, usw.
- Die Hacker dringen in die Systeme ein, nutzen diese Daten für kriminelle Zwecke, greifen in die Steuerung des Unternehmens ein, greifen Daten ab und legen den Betrieb lahm

Cyber: Aktueller Status Quo

Fallbeispiel GWG Wohnungsbaugesellschaft



Süddeutsche Zeitung

18. November 2020, 15:31 Uhr Cyber-Kriminalität

Hacker erpressen die GWG Wohnungsbaugesellschaft

Sie fordern Geld, damit der Konzern wieder Zugriff auf seine IT-Systeme bekommt. Seit fast einer Woche können die Mitarbeiter unter anderem nicht auf ihre E-Mails zugreifen.

Von Andreas Schubert

Es ist der Albtraum einer jeden Firma: Die Computersysteme sind von Hackern blockiert worden, um sie wieder zu entsperren soll das Unternehmen ein Lösegeld zahlen. Genau das ist der GWG Wohnbaugesellschaft München passiert. Vor einer Woche, in der Nacht auf den 12. November, haben Hacker das Computersystem der GWG lahmgelegt. Bei dem Cyber-Angriff wurde ein Großteil der IT-Systeme und Daten verschlüsselt, auch Backup-Server und Datensicherungen auf Festplatten sind betroffen. Die Folge: Mitarbeiter der GWG können seit Donnerstag nicht mehr auf das System zugreifen, also zum Beispiel auch nicht auf ihre geschäftlichen E-Mails.

Der Angriff erfolgte nach Angaben der GWG und der für Cyber-Kriminalität zuständigen Generalstaatsanwaltschaft Bamberg mittels einer sogenannten "Ransomware". Ransom ist das englische Wort für Lösegeld. Wie die GWG am Mittwoch mitteilte, handelte es sich um einen "hochprofessionellen Angriff mit dem Ziel, das Opfer zu erpressen". Als Gegenleistung behaupteten die anonymen Angreifer, sie würden die IT-Systeme entschlüsseln.

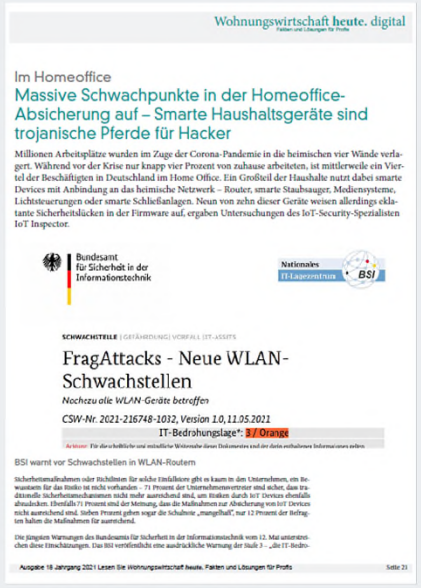
Die GWG hat inzwischen Strafanzeige gestellt. Sie geht nach eigener Aussage aber derzeit davon aus, dass sie mit eigenen Mitarbeiterinnen und Mitarbeitern und externen Spezialdienstleistern die wesentlichen Datenbestände wiederherstellen kann. Man stehe in engem Austausch mit den auf Cybercrime spezialisierten Ermittlungsbehörden. In wie vielen Tagen ein Zugriff auf welche IT-Systeme und Daten wieder möglich sein wird, sei noch Gegenstand der Analyse und der Arbeiten.

Die GWG hat einen der vom Bundesamt für Sicherheit in der Informationstechnik qualifizierten Dienstleister beauftragt, eine umfassende forensische Analyse zu betreiben und das Unternehmen beim Wiederaufsetzen und Wiederherstellen der Systeme zu unterstützen. Den laufenden Geschäftsbetrieb wird die GWG soweit wie möglich aufrechterhalten. Für ihre Mieter sowie für ihre Geschäftspartner sind die GWG-Mitarbeiter weiterhin telefonisch erreichbar. Die Hausmeister seien weiter vor Ort und kümmerten sich um die Belange der Mieter.

Welche Forderungen an die GWG gestellt wurden, darüber machen die Ermittler keine Angaben. Neben der Polizei München ist die in Bamberg ansässige Zentralstelle Cybercrime Bayern (ZCB) mit dem Fall betraut. Nach deren Angaben haben in den vergangenen Jahren die Fälle von Internetkriminalität massiv zugenommen. Während im Gründungsjahr 2015 noch 478 Verfahren gegen bekannte und unbekannte Beschuldigte erfasst worden seien, habe die ZCB im Jahr 2019 insgesamt 14 198 Ermittlungsverfahren eingeleitet. Die Fälle des ZCB reichen von Hackerangriffen über Betrug mit falschen Internetshops bis hin zum Handel mit Waffen, Drogen und Falschgeld im Darknet. Anfang Oktober dieses Jahres hat unter dem Dach der ZCB auch das Zentrum zur Bekämpfung von Kinderpornografie und sexuellem Missbrauch im Internet seine Arbeit aufgenommen.

Cyber: Aktueller Status Quo

Gefahren - Beispiel Homeoffice



Wohnungswirtschaft heute. digital

Im Homeoffice

Massive Schwachpunkte in der Homeoffice-Absicherung auf – Smarte Haushaltsgeräte sind trojanische Pferde für Hacker

Millionen Arbeitsplätze wurden im Zuge der Corona-Pandemie in die heimischen vier Wände verlagert. Während vor der Krise nur knapp vier Prozent von zuhause arbeiteten, ist mittlerweile ein Viertel der Beschäftigten in Deutschland im Home Office. Ein Großteil der Haushalte nutzt dabei smarte Devices mit Anbindung an das heimische Netzwerk – Router, smarte Staubsauger, Mediensysteme, Lichtsteuerungen oder smarte Schließanlagen. Neun von zehn dieser Geräte weisen allerdings eklatante Sicherheitslücken in der Firmware auf, ergaben Untersuchungen des IoT-Security-Spezialisten IoT Inspector.

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

FragAttacks - Neue WLAN-Schwachstellen

Nochezu alle WLAN-Geräte betreffen

CSW-Nr. 2021-216748-1032, Version 1.0,11.05.2021

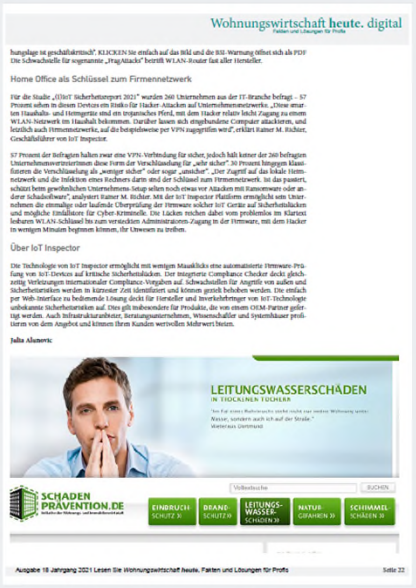
IT-Bedrohungslage*: 3 / Orange

BSI warnt vor Schwachstellen in WLAN-Routern

Sicherheitsmaßnahmen oder Richtlinien für solche Einfallstore gibt es kaum in den Unternehmen, ein Bewusstsein für das Risiko ist nicht vorhanden – 71 Prozent der Unternehmensvertreter sind sicher, dass traditionelle Sicherheitsmechanismen nicht mehr ausreichend sind, um Risiken durch IoT Devices ebenfalls abzudecken. Ebenfalls 71 Prozent sind der Meinung, dass die Maßnahmen zur Absicherung von IoT Devices nicht ausreichend sind. Sieben Prozent gehen sogar die Schalbreite „mangelhaft", nur 12 Prozent der Befragten halten die Maßnahmen für ausreichend.

Die jüngsten Warnungen des Bundesamts für Sicherheit in der Informationstechnik vom 12. Mai unterstreichen diese Einschätzungen. Das BSI veröffentlicht eine ausdrückliche Warnung der Stufe 3 – „die IT-Bedro-

Ausgabe 18 Jahrgang 2021 Lesen Sie Wohnungswirtschaft heute. Fakten und Lösungen für Profis Seite 21



Wohnungswirtschaft heute. digital

hungslage ist geschäftskritisch", KLICKEN Sie einfach auf das Bild und die BSI-Warnung öffnet sich als PDF

Die Schwachstelle für sogenannte „FragAttacks" betrifft WLAN-Router fast aller Hersteller.

Home Office als Schlüssel zum Firmennetzwerk

Für die Studie „(U)IoT Sicherheitsreport 2021" wurden 260 Unternehmen aus der IT-Branche befragt – 57 Prozent sehen in diesen Devices ein Risiko für Hacker-Attacken auf Unternehmensnetzwerke. „Diese smarten Haushalts- und Heimgeräte sind ein trojanisches Pferd, mit dem Hacker relativ leicht Zugang zu einem WLAN-Netzwerk im Haushalt bekommen. Darüber lassen sich eingebundene Computer attackieren, und letztlich auch Firmennetzwerke, auf die beispielsweise per VPN zugegriffen wird", erklärt Rainer M. Richter, Geschäftsführer von IoT Inspector.

57 Prozent der Befragten halten zwar eine VPN-Verbindung für sicher, jedoch hält keiner der 260 befragten Unternehmensvertreterinnen diese Form der Verschlüsselung für „sehr sicher". 30 Prozent bingegen klassifizieren die Verschlüsselung als „weniger sicher" oder sogar „unsicher". „Der Zugriff auf das lokale Heimnetzwerk und die Infektion eines Rechners darin sind der Schlüssel zum Firmennetzwerk. Ist das passiert, schützt beim gewöhnlichen Unternehmens-Setup selten noch etwas vor Attacken mit Ransomware oder anderer Schadsoftware", analysiert Rainer M. Richter. Mit der IoT Inspector Plattform ermöglicht sein Unternehmen die einmalige oder laufende Überprüfung der Firmware solcher IoT Geräte auf Sicherheitslücken und mögliche Einfallstore für Cyber-Kriminelle. Die Lücken reichen dabei vom problemlos im Klartext lesbaren WLAN-Schlüssel bis zum versteckten Administratoren-Zugang in der Firmware, mit dem Hacker in wenigen Minuten beginnen können, ihr Unwesen zu treiben.

Über IoT Inspector

Die Technologie von IoT Inspector ermöglicht mit wenigen Mausklicks eine automatisierte Firmware-Prüfung von IoT-Devices auf kritische Sicherheitslücken. Der integrierte Compliance Checker deckt gleichzeitig Verletzungen internationaler Compliance-Vorgaben auf. Schwachstellen für Angriffe von außen und Sicherheitsrisiken werden in kürzester Zeit identifiziert und können gezielt behoben werden. Die einfach per Web-Interface zu bedienende Lösung deckt für Hersteller und Inverkehrbringer von IoT-Technologie unbekannte Sicherheitsrisiken auf. Dies gilt insbesondere für Produkte, die von einem OEM-Partner geliefert werden. Auch Infrastrukturanbieter, Versorgungsunternehmen, Wissenschaftler und Systemhäuser profitieren von dem Angebot und können ihren Kunden wertvollen Mehrwert bieten.

Julia Alunovic

LEITUNGSWASSERSCHÄDEN

IN TROCKENEN TÜCHERN

SCHADEN PRÄVENTION.DE

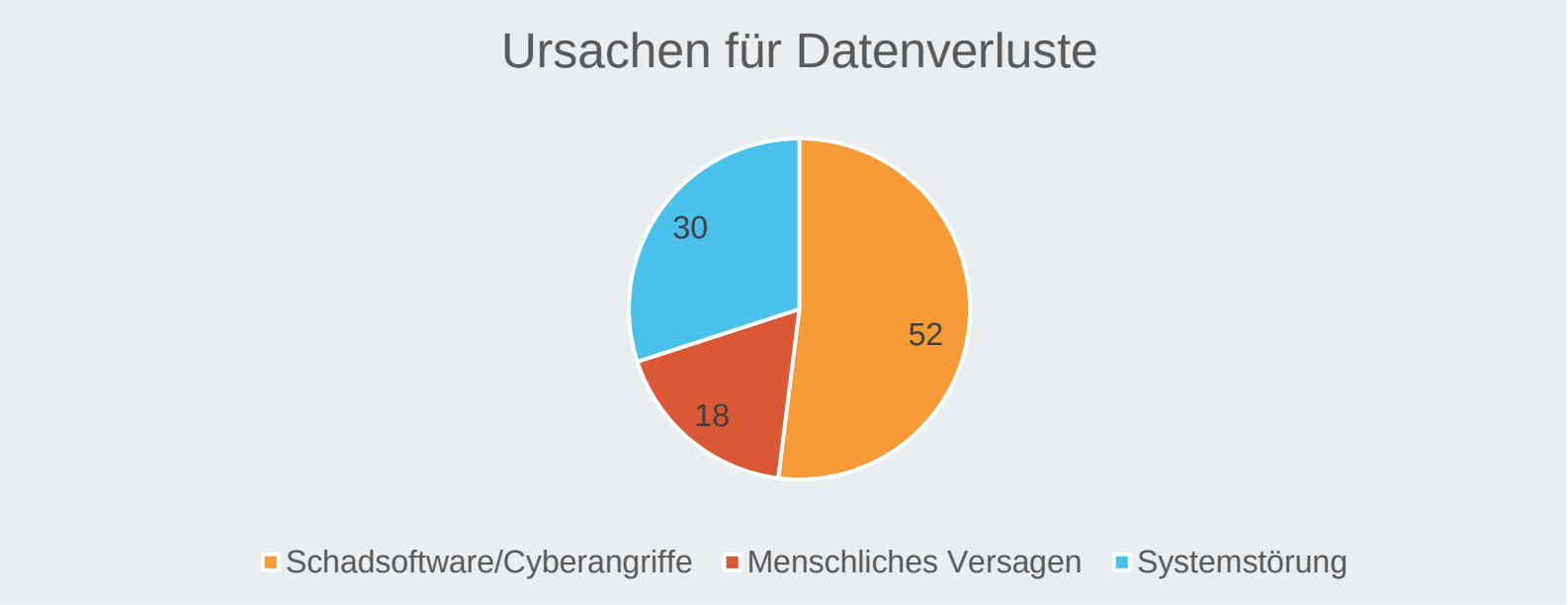
EINBRUCH-SCHUTZ » BRAND-SCHUTZ » LEITUNGS-WASSER-SCHÄDEN » NATUR-GEFAHREN » SCHIMMEL-SCHÄDEN »

Ausgabe 18 Jahrgang 2021 Lesen Sie Wohnungswirtschaft heute. Fakten und Lösungen für Profis Seite 22

Verständnis für Strukturen des Cyberkrisenmanagements

- **Risiken**
- **Wer sind die Angreifer**
- **Phasen der Angriffe**

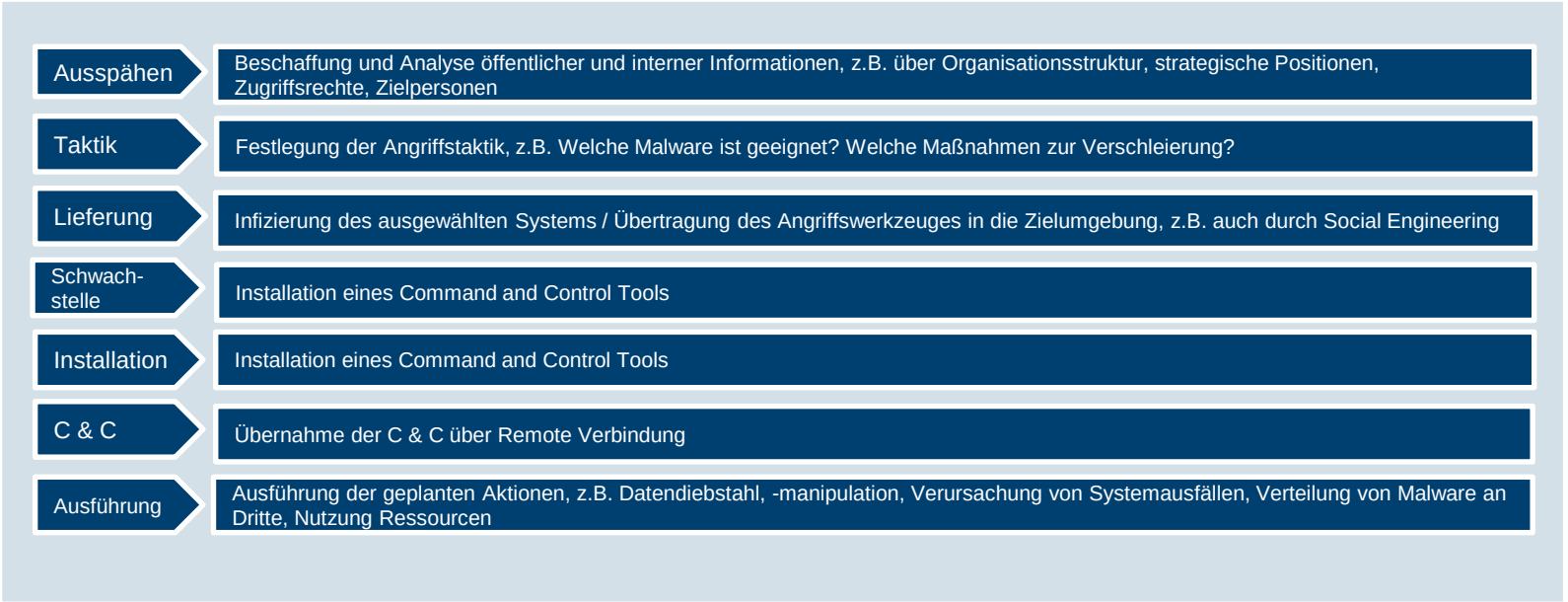
Verständnis für die Strukturen: Cyber-Risiken



Verständnis für die Strukturen: Wer sind die Angreifer?

Bedrohungsmatrix	Cyber-Crime	Script-Kiddies	Cyber-Spionage	Hacktivismus	Interne Täter
Motivation	Geld	Spaß, Neugier	strategisch	Ethik, Politik	Rache, Geldnot
Zielauswahl	individuell, zufällig	zufällig, politisch	individuell	ideologisch, politisch	Arbeitgeber
Organisation	sehr hoch	teilweise	sehr hoch bis perfekt	strukturiert	kaum
Kompetenz	hoch	gering bis hoch	sehr hoch	mittel bis hoch	hoch, Insiderwissen

Verständnis für die Strukturen: Phasen des Cyber-Angriffes



Arten von

Cyber-Bedrohungen

Cyber-Bedrohung: Social Engineering

- Einflussnahme auf einen Mitarbeiter mit dem Ziel, an geheime Daten zu gelangen
- In der Regel geschieht dies telefonisch. Der Anrufer gibt z.B. vor, ein Kollege aus der IT-Abteilung zu sein und bittet um das Passwort des Mitarbeiters

Cyber-Bedrohung: DoS-Attacke

- „DoS“ steht für Denial of Service (Dienstverweigerung)
- Angriffe auf ein Computersystem, die durch gezielte Überlastung des Systems dessen Funktion stören oder außer Kraft setzen

Cyber-Bedrohung: Malware

- Zu dieser bösartigen Software gehören Computerviren, Spyware, Trojanische Pferde, Würmer und alle anderen Programme oder Dateien, die den Computer schädigen können
- Malware wird in der Regel durch scheinbar legitime Downloads oder Anhänge in E-Mails verbreitet

Cyber-Bedrohung: Phising

- Phishing (Neologismus von fishing, engl. für „Angeln“)
- Bei dieser Art von Cyber Bedrohung werden gefälschte eMails von scheinbar legitimen Quellen versendet, um an Informationen wie Kreditkartendaten oder Passwörter zu gelangen

Cyber-Bedrohung: SQL-Injection

- SQL=**S**tructured **Q**uery **L**anguage; dt.: **strukturierte Abfragesprache**
- Der Angreifer schleust eigene Befehle in die SQL-Datenbank des Systems
- Das spätere automatische Ausführen dieser Befehle soll den Zugriff auf die Datenbank ermöglichen. Der Hacker gelangt so an sensible Daten oder erhält unter Umständen sogar die Kontrolle über den Server

Cyber-Bedrohung: Physischer Zugang

- Der Angreifer verschafft sich Zutritt zum Gebäude
- Installieren von Hardware oder Abgreifen von Daten an nicht gesicherten Rechnern

Cyber-Auswirkungen

Cyber-Auswirkungen: Eigenschäden

- Kosten für die Wiederherstellung der Daten, der Systeme und des Netzwerkes nach einem Hackerangriff
- Kosten für IT-Forensiker, die die Sachverhalte schnell aufklären und gerichtsverwertbar dokumentieren
- Kosten für Krisenmanagement und PR-Maßnahmen nach einem Hackerangriff
- Kosten für die Verbesserung der Sicherheit nach einem Hackerangriff

Cyber-Auswirkungen: Haftpflichtschäden

- Verstoß gegen gesetzliche oder vertragliche Bestimmungen zum Datenschutz
- Verstoß gegen Geheimhaltungspflichten
- Weiterverbreitung von Computerviren an Dritte
- Verletzung von Persönlichkeitsrechten nach einem Hacker-Angriff
- Verstoß gegen E-Payment-Vereinbarungen

Cyber-Auswirkungen: Vertrauensschäden

- z.B. Eingriffe in die Buchhaltung, die zu Kontoabbuchungen führen
- Entgangener Gewinn nach Verrat oder Ausspähung von Betriebs- und Geschäftsgeheimnissen
- Mitarbeiter werden getäuscht und bezahlen z.B. eine manipulierte Rechnung, die per eMail zugeschickt wurde

Cyber-Auswirkungen: Ertragsausfall

- Kosten durch Stilllegung der Produktion / des Unternehmens

Cyber-Auswirkungen: Schäden - Fallszenario

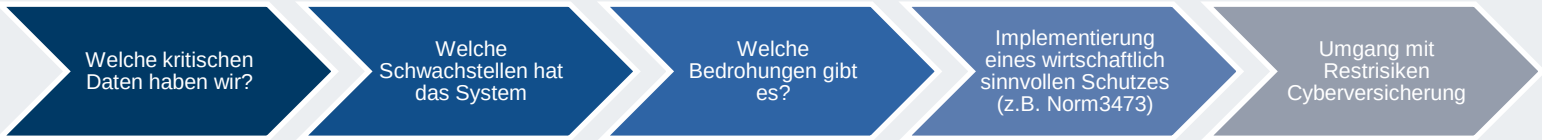
Schadenszenario: Virus legt Hochregellager lahm

Auswirkungen:

- BU-Schaden aufgrund der kontrollierten Systemabschaltung:	300.000 EUR
- Dekontamination infizierter Daten:	45.000 EUR
- Wiederherstellung der Daten aus Back-Up Sicherungen:	15.000 EUR
- Manuele Auslagerung und Neuerfassung eines Teils der Lagerware:	160.000 EUR
- Vertragsstrafen aufgrund verspäteter Auslieferung:	175.000 EUR
	695.000 EUR

Die Cyber-Versicherung

Cyber: Von schützenswerten Daten zur Cyber-Versicherung



Die Cyber-Versicherung: Mögliche Inhalte

- Benachrichtigungskosten
- Call-Center Kosten
- Kundenbindungsaktionen
- Vertragsstrafen der Payment Card Industry
- Kreditkartenmonitoring
- Behördliche Verfahren
- Entschädigungen mit Strafcharakter, Bußgelder, etc.
- Cyber-Diebstahl und Cyber-Betrug
- Vertragsstrafen im Rahmen der BU