Angriffe aus dem Darknet abgewehrt

Wie man sich bei CyberCrime vor Schaden schützt

E-Day:17

Wien, 12. April 2017

Ing. Alexander Punzl, IRM-KOTAX Versicherungssysteme GmbH

In Zusammenarbeit mit der Erichsen GmbH

Erichsen

irm kotax VERSICHERUNGSSYSTEME

Themen

- Cybercrime: Versicherbare Risiken im Netz
- Hot Case: Wenn der Schaden passiert ist
- Learnings: Internationale Erfahrungen

- Februar 2016
Cyber-Angriffe auf mehrere deutsche Krankenhäuser

Ein Virus hat seit Mittwoch (10.02.2016) das System des Lukaskrankenhauses in Neuss lahmgelegt. OPs mussten verschoben und schwere Notfälle in andere Kliniken delegiert werden. Offenbar ist das kein Einzelfall. Fünf weitere Häuser in NRW sollen in letzter Zeit Opfer von Cyberattacken gewesen sein.

Wir haben IT-Experten verschiedener Krankhäuser dazu befragt. Diese gehen von einer Schadenhöhe von mindestens 1 Mio. Euro aus.

Seit drei Tagen legt ein unglaublich raffiniert programmiertes Computervirus die zentrale EDV des Neusser Lukaskrankenhauses lahm. „Wir sind so technologisch wieder auf dem Stand von vor 15 Jahren“, sagt Kliniksprecher. Das bedeutet für den Krankenhausbetrieb deutlichen Mehraufwand. Die Personalstärke wurde erhöht. Beispiel Notaufnahme: „Bis vor drei Tagen hatten wie alle Patientendaten im Rechner. Man konnte die Patienten per Drag&Drop den Behandlungsräumen zuweisen, man hatte sofort Zugriff auf alle Daten. Auch bei Patienten, die schon öfter im Lukaskrankenhaus waren. Dieser Zugriff fehlt jetzt“, erklärt Dr. Klaus Reinarzt, Leiter der Zentralambulanz. Für Laborberichte muss er zurzeit einen Zettel „händisch“ ausfüllen, vorher ging alles über PC automatisch.
„Für uns bedeutet der Ausfall auch mehr Arbeit“, berichtet Dr. Ansgar Müller-Chorus, Leiter des Zentrallabors. Mit EDV gingen die Anforderungen aus den Abteilungen direkt in die Analysemaschinen. „Jetzt müssen wir jeder Maschine jede Analyse manuell eingeben“.
Und auch die Befunde gehen nun nicht mehr automatisch in die digitale Patientenakte. Jede Maschine druckt ihre Befunde einzeln aus.

Quellen:
www.heise.de
www.express.de
www.wdr.de
Erichsen GmbH

- November 2016

Rosa Riese mit blauem Auge davon gekommen

Nichts ging mehr für viele Telekom-Kunden am Wochenende: Telefon tot, Internet ebenfalls unterbrochen. Fast eine Million Haushalte waren betroffen. Ursache der bundesweiten Störung waren aber keine Ausfälle der Netzinfrastruktur selbst, vielmehr waren es die von der Telekom bereitgestellten Speedport-DSL-Router der Kunden, die plötzlich ihren Dienst versagten.

Bisher unbekannte Hacker hatten weltweit versucht, eine Sicherheitslücke in DSL-Routern auszunutzen, um Schadsoftware auf den Geräten zu installieren. Der Netzausfall der Telekom war dabei mutmaßlich gar nicht beabsichtigt sondern vielmehr ein unerwünschter jedoch erheblicher Nebeneffekt der Attacke. Die Schwachstelle im Fernwartungsprotokoll (genannt TR-069/TR-064) erlaubte es den Hackern, Zugriff auf die Speedport-Router über das Internet zu nehmen und Funktionen der Fernwartungsschnittstelle aufzurufen. Der vorgesehene Angriff versagte dabei: eine endgültige Kontrolle über die Router konnte nicht zuletzt wegen einer schlampig programmierten Schadsoftware nicht erlangt werden. Trotzdem war der Schaden erheblich, denn die Router versagten nach dem Angriffsversuch den Dienst.

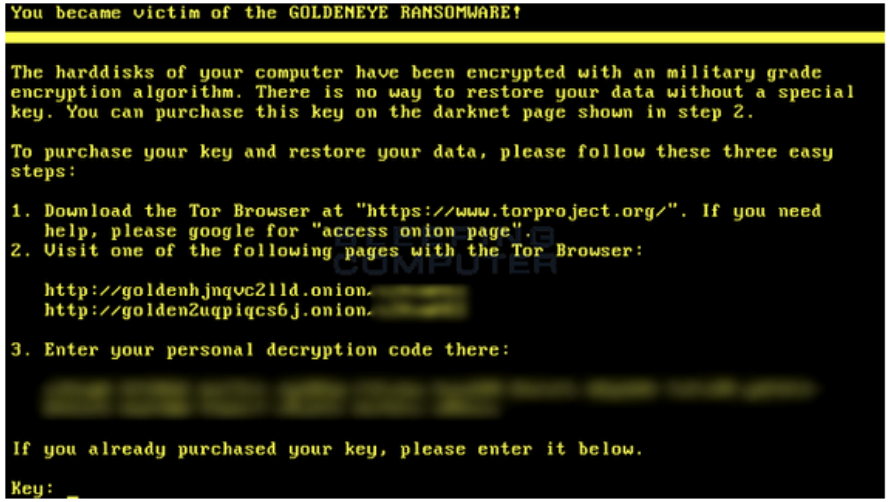
- Dezember 2016

Quellen:
www.heise.de
www.t.online.de

Polizei warnt

Neuer Erpressertrojaner "Goldeneye" verbreitet sich in Deutschland rasant

Eine als Bewerbung getarnte E-Mail wird derzeit verstärkt an Unternehmen in Deutschland geschickt, warnt die Polizei. In ihrem Anhang verschicken Cyber-Kriminelle einen neuen Erpresser-Trojaner namens "Goldeneye". Derzeit gibt es noch kaum Schutz vor dem Schädling – und auch kein Entschlüsselungstool.



Wenn der Erpressungs-Trojaner Goldeneye zugeschlagen hat, sind die Daten vorerst in der Gewalt der Kriminellen. Den Schlüssel wollen sie erst rausrücken, wenn Opfer das Lösegeld in Höhe von 1,33284506 Bitcoin (rund 940 Euro) bezahlen.

Goldeneye hat es in erster Linie auf Personalabteilungen in Deutschland abgesehen. Doch wer die folgenden Tipps befolgt und in Unternehmen verbreitet, kann eine Infektion verhindern oder den Verschlüsselungsvorgang noch frühzeitig stoppen, sodass nicht alle Daten betroffen sind. Und Vorsicht: Goldeneye verbreitet sich derzeit rasant.

Im Schadenfall fallen Kosten an für:

- **Schadenersatzansprüche Dritter:**
  - **Rechtschutzfunktion / Anspruchsabwehr**
  - **Befriedigung berechtigter**

- **Wiederherstellungskosten Daten und Netzwerke**

- **Ertragsausfall durch Umsatzverluste**
- **Mehrkosten zur provisorischen Aufrechterhaltung oder beschleunigen Wiederherstellung des Betriebs**

- **Erpressungsgelder**

- **Kosten für Information betroffener Dateninhaber nach Datenschutzvorfall**
- **Kosten IT Forensik**
- **Kosten Rechtsberatung**
- **Kosten PR-Berater**
- **PCI Vertragsstrafen**

Risiken aus IT- / web-gestützter Steuerung von Produktion, Prozessen und Transaktionen

Für welche Unternehmen ist eine Cyber- Versicherung wichtig?

Grundsätzlich für jedes Unternehmen, das

wichtige **Prozesse** und Transaktionen IT- und / oder Web-gestützt steuert

Schwerpunkt: Cyber
Risiken aus IT- / web-gestützter Steuerung von Produktion, Prozessen und Transaktionen

und / oder

sensible **Daten** (personenbezogene oder sonstige vertrauliche) seiner Kunden, Mitarbeiter, Patienten, Vertragspartner speichert, bearbeitet oder verwaltet.

Schwerpunkt: Datenschutz
Risiken aus Verarbeitung und Speicherung sensibler Daten

und / oder

Über IT-Systeme **Vermögenswerte** verwaltet (z.B. Online-Banking)

Schwerpunkt: Vermögen
Risiken elektronischem Zugriff auf Vermögenswerte

Risiken aus IT- / web-gestützter Steuerung von Produktion, Prozessen und Transaktionen

Katastrophenszenario:
Gezielte Verfälschung und Infizierung von Datensätzen

Bei einem weitreichenden Angriff auf die Serverinfrastruktur wäre es denkbar, dass das Unternehmen keine integren Datensätze mehr besitzt. Kurz: Es weiß nicht mehr, welche Daten zu welchem Kunden gehören.

Die Backups sind ebenfalls betroffen, weil der Angreifer diesen "Totalschaden" beabsichtigte und den Backup-Prozess manipulierte.
Hier wäre ein besonders langer Ausfallzeitraum zu berücksichtigen; es müssten Daten von Papierausdrucken (Mikrofiche?) re-digitalisiert werden.

> - Die Web-Applikation wurde sechs Monate zuvor angegriffen, mehrere Serverskripte wurden verändert, um Daten vor dem Speichern in die sowie nach dem Auslesen aus der Datenbank zu verschlüsseln. Die bedeutete eine Art "on-fly"-Patching, das für die Nutzer der Applikation unsichtbar war.
> - Dabei wurden nur einige der wichtigsten Felder der Datenbanktabellen verschlüsselt (vermutlich um die Performance der Web-Applikation nicht zu sehr zu beeinträchtigen). Alle bereits vorhandenen Databank-Inhalte wurden auf die gleiche Weise verschlüsselt.
> - Der Verschlüsselungs-Key wurde auf einem externen Server gespeichert und nur per HTTPS zugänglich gemacht (vermutlich um ein Abfangen des Schlüssels durch Traffic Monitoringsysteme zu verhindern).
> - Sechs Monate lang warteten die Hacker still, während Backups mit der kompromittierten Version der Datenbank überschrieben wurden. Am Tag X entfernten die Hacker den Verschlüsseltungs-Key vom externen Server. Damit wurde die Datenbank unbrauchbar, die Website funktionierte nicht mehr und die Hacker verlangten Lösegeld für den Verschlüsselungs-Key.

Datenpanne

- Durchschnittliche Kosten pro Datensatz € 50,-- - € 146,--
  - Entgangener Umsatz
  - Ausgaben für die Aufdeckung
  - Interne Aufarbeitung
  - Benachrichtigung der Betroffenen
  - Benachrichtigung Datenschutzbehörde
- Die Anzahl der Datensatzverlust je Datenpanne liegt häufig zwischen 3.750 und 90.000

Grundstruktur der Cyber- Versicherung

Cyber-Vorfall

Haftpflicht

- Schadenersatzansprüche Dritter:
  - Rechtschutzfunktion / Anspruchsabwehr
  - Befriedigung berechtigter

Eigenschäden

- Wiederherstellungskosten Daten und Netzwerke
- Ertragsausfall durch Umsatzverluste
- Mehrkosten zur provisorischen Aufrechterhaltung oder beschleunigen Wiederherstellung des Betriebs
- Optional: Betriebsunterbrechung infolge Cloud – Ausfall
- Optional: Cyber-Diebstahl (Außentäter)
- Nach Vereinbarung: Erpressungsgelder

Kostenpositionen

- Kosten für Information betroffener Dateninhaber nach Datenschutzvorfall
- Kosten IT Forensik
- Kosten Rechtsberatung
- Kosten PR-Berater
- PCI Vertragsstrafen

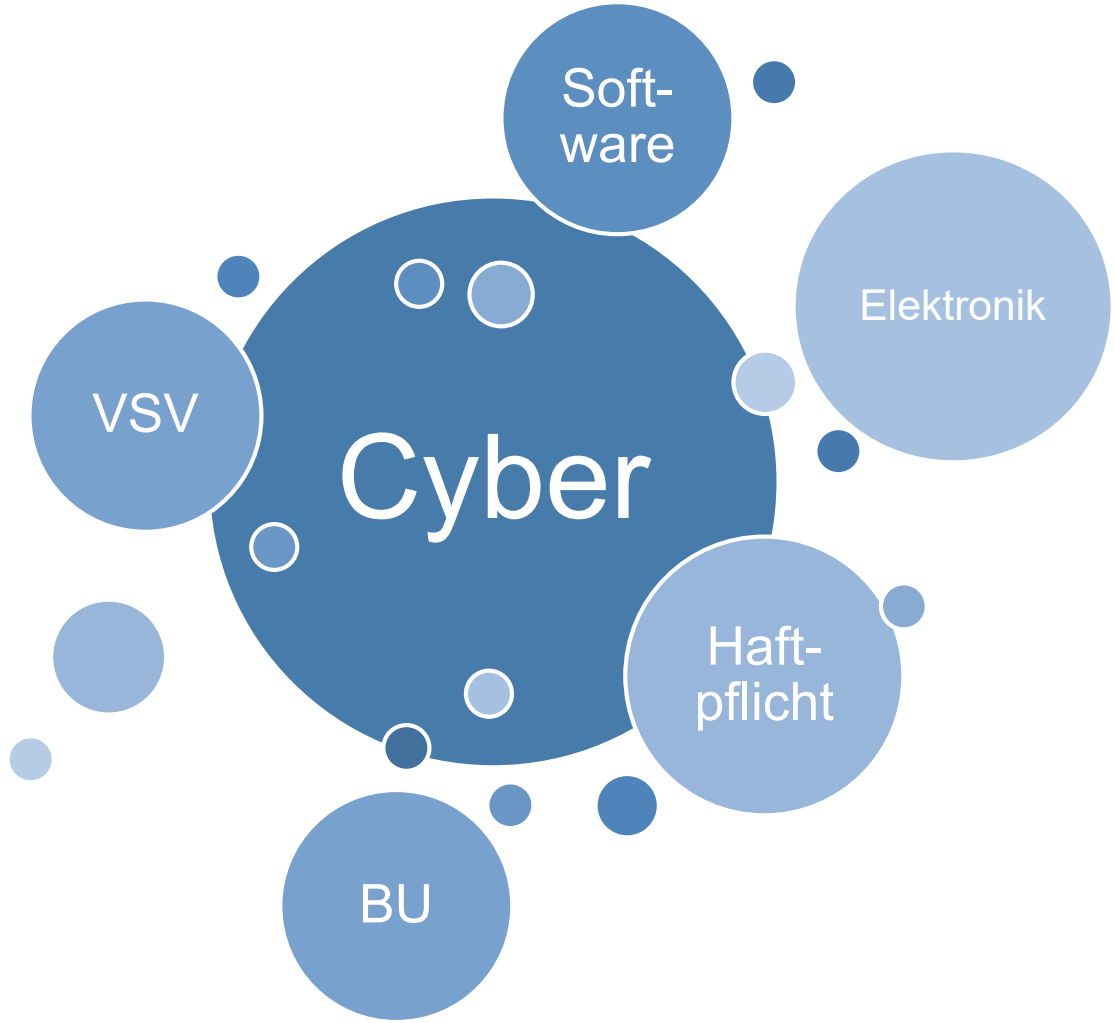
Erichsen

Überschneidungen mit anderen Versicherungssparten (1)

Cyber-Risiken werden nur ausschnittsweise und begrenzt über traditionelle Haftpflicht-, Sach- oder Vertrauensschadenversicherungen abgedeckt, da letztere aus einer ‚nicht digitalen Zeit' stammen. Risiken aus dem Netz wurden in die traditionellen Deckungen nicht oder nur punktuell aufgenommen.

Der Versicherungsschutz für Cyber-Risiken in diesen Sparten ist unzureichend, da

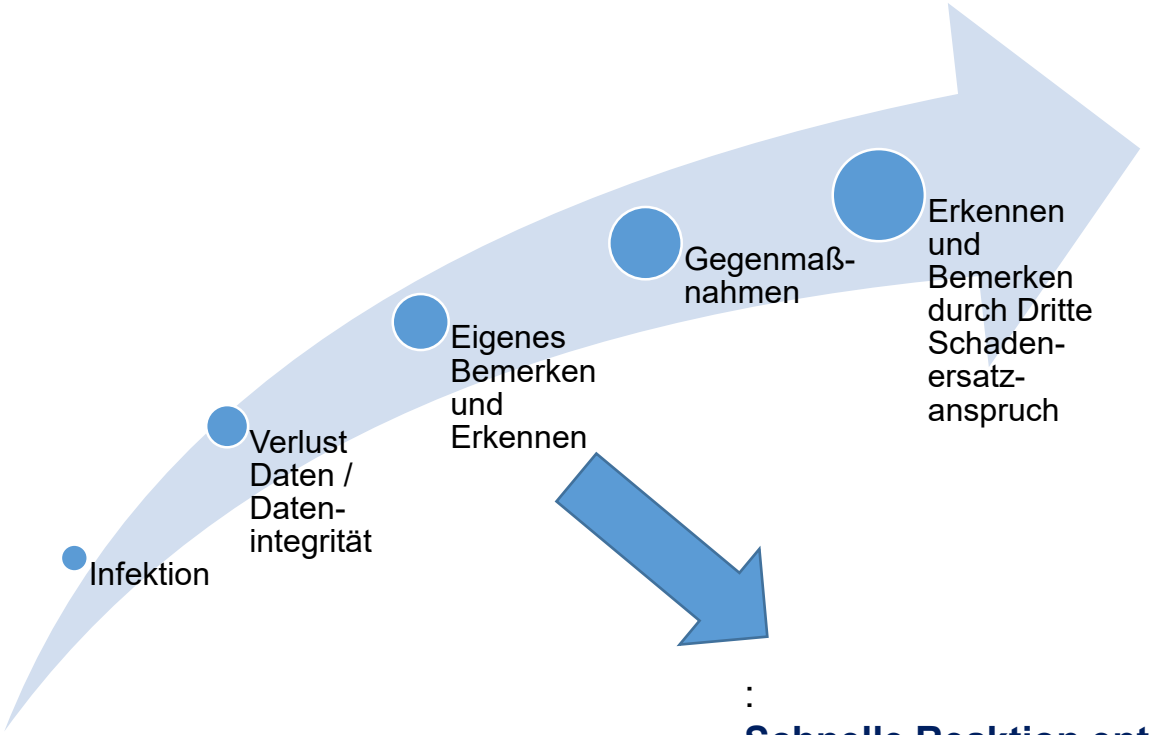
- weitreichende Ausschlüsse für relevante Risiken bestehen
- jeweils andere Versicherungsfall-Definitionen zu berücksichtigen
- im Schadenfall stets mehrere Versicherer zu involvieren sind.



Überschneidungen mit anderen Versicherungssparten (2)

	Sach / TV	Haftpflicht	VSV	Cyber
		☹		☺
Benachrichtigungskosten im Datenschutzvorfall	☹	☹	☹	☺
		☹		☺
Kosten für IT-Forensik	☹	☹	bedingt	☺
	☹	☹		☺
Cyberbezogene Erpressung / Bedrohung	☹	☹	☹	☺
	☹	☹	☹	
Diebstahl Geld oder Vermögenswerte in elektronischer Form	☹	☹	bedingt	bedingt
	☹	☺	☹	☺
Forderungen der PaymentCard-Industrie	☹	☹	☹	☺
	☹		☹	
Ansprüche Dritter aus Verletzung Rechte des geistigen Eigentums	☹	bedingt	☹	bedingt

CYBER RISKS
Typische Versicherungsbausteine :
Assistance-Bausteine



:

Schnelle Reaktion entscheidend

It-Forensik, Krisenberatung, Rechtsrat
Versicherer stellt Expertennetzwerk

- VERSICHERER

Erichsen

CYBER RISKS
Ausblick Markt Gewerbe Industrie

Ausblick - Schätzungen

- Zur Zeit ca. 6.000 Abschlüsse (überwiegend in Ende 2015 und 2016)
- Große Anzahl Anbahnungen = Interesse wächst exponentiell
- Marktprämie Deutschland z.Zt. € 30 Mio., Tendenz steigend (Schätzung KPMG)
- USA Marktprämie USD 3 Mrd.
- Potential € 20 Mrd. Prämie in 15 Jahren

Erichsen

Markttrends

- 2.000 – 10.000 Euro pro Mio. Euro Deckungssumme
- Durchschnittsprämien zwischen € 490,-- und € 5.000,--
- Selbstbehalt mind. € 1.000,--
- Schadensfälle nehmen zu

IM NOTFALL …

„Cyber-Versicherung - bald so selbstverständlich wie eine Feuer-Versicherung“

Kontakt:

Herr Ing. Alexander Punzl

T 01 5036233 93 M 0664 8134067 a.punzl@irm-kotax.com

Vielen Dank

Haben Sie noch Fragen?