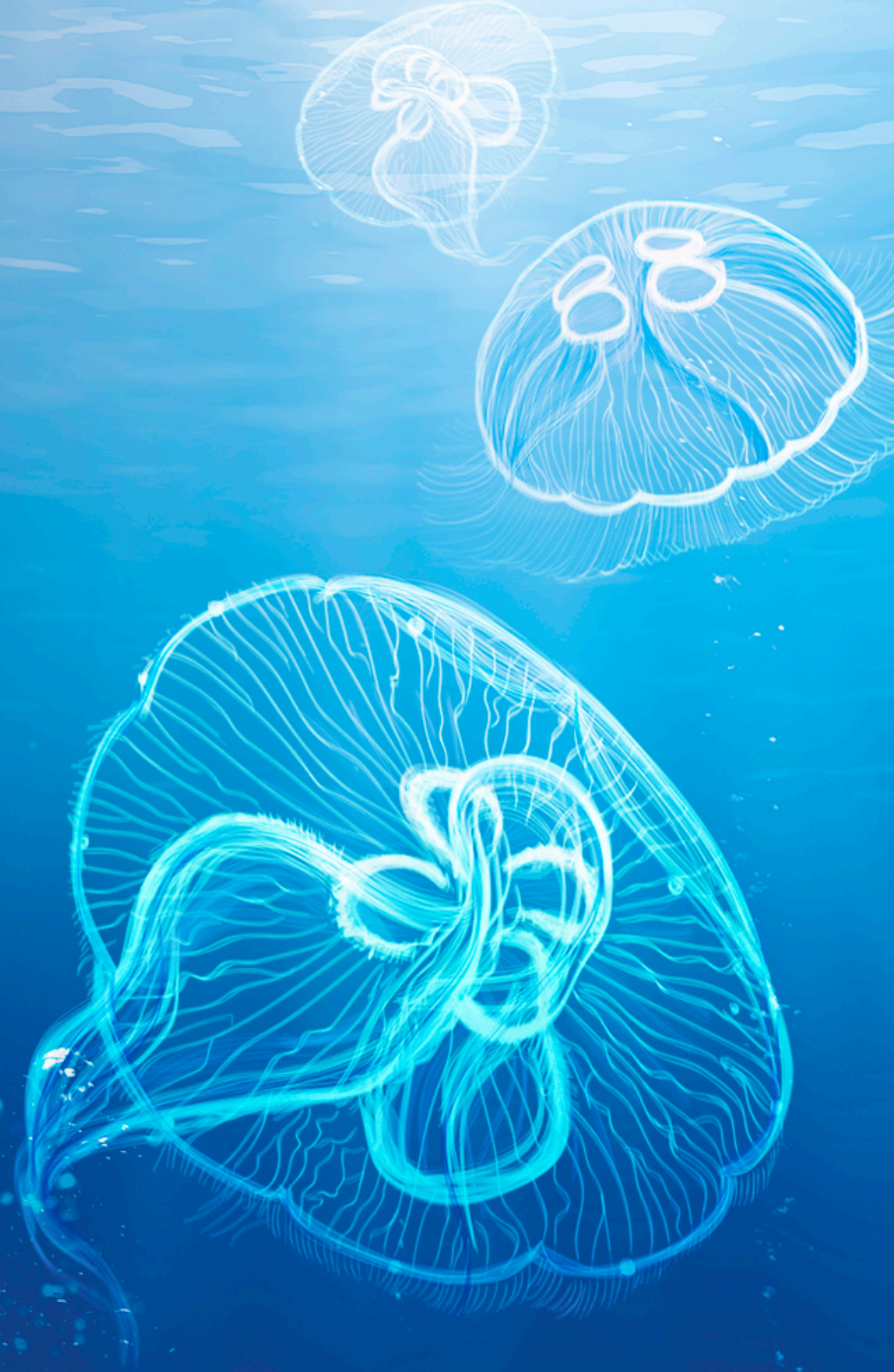




# Das Geld der Anderen

**Compliance Solution Day 2019**

—  
Wien, 25. September 2019





**SAP**

**Oracle**

**FIS Global**

**Intuit Inc.**

**Cerner Corporation**

**FI Serv**

**Microsoft**

**SS&C Technologies**

**Infor**

**Constellation Software**


Quelle: <https://www.appsruntheworld.com/top-10-erp-software-vendors-and-market-forecast/>

# 50,000 companies exposed to hacks of 'business critical' SAP systems: researchers

Jack Stubbs

4 MIN READ



LONDON (Reuters) - Up to 50,000 companies running SAP software are at greater risk of being hacked after  found new ways to exploit vulnerabilities of systems that haven't been properly protected and published the tools to do so online.

Quelle: <https://www.reuters.com/article/us-sap-security/50000-companies-exposed-to-hacks-of-business-critical-sap-systems-researchers-idUSKCN1S80VJ>



# Die Vorbereitung

Öffentliche Quellen und Informationen als Hinweise

# Familienunternehmen

International tätig, Jahresbericht 2018



Die Einzelabschlüsse werden von den Konzernunternehmen überwiegend mittels Microsoft Dynamics NAV erstellt, weitere im Einsatz befindliche ERP-Systeme sind proAlpha und SAP. Die Daten werden elektronisch in einem einheitlichen Format übermittelt und vom Konzernrechnungswesen in die Konsolidierungssoftware (IDL Konsis) eingespielt. Für die rechnungslegungsbezogenen IT-Systeme sind Zugriffsberechtigungen definiert, um zu gewährleisten, dass sensible Daten vor nicht genehmigtem Zugriff, Verwendung und Veränderung geschützt sind.

# Öffentliches Unternehmen

## Geschäftsbericht 2018



ein  
Auslöser für das Projekt war die als Basis für eine künftige S4/HANA-Implementierung notwendige Einführung des neuen Hauptbuches und des zentralen Geschäftspartners im SAP. Das Projekt wurde dazu genutzt, neben einer Kontenplanreorganisation in mehreren Modulen nicht mehr verwendete Einstellungen, Organisationseinheiten, Stamm- und Bewegungsdaten zu bereinigen. Weitere Schwerpunkte waren die Zusammenführung in- und ausländischer Gesellschaften in einen Mandanten und die Einführung bestimmter neuer Funktionalitäten. Die Produktivmigration erfolgte im Jänner 2018, womit alle Buchungen seit 01.01.2018 im neuen System stattfinden.



# ATX Konzern

## Geschäftsbericht 2018



Kontrollmaßnahmen in Bezug auf die IT-Sicherheit stellen in diesem Zusammenhang einen Eckpfeiler des Internen Kontrollsystems dar. So wird die Trennung bzw. Segmentierung von sensiblen Tätigkeiten durch eine generell restriktive Vergabe von IT-Berechtigungen unterstützt. Für die Rechnungslegung in den einzelnen Konzernunternehmen wird im Wesentlichen die Software SAP verwendet. Die Ordnungsmäßigkeit dieser SAP-Systeme wird u. a. auch durch direkt im System eingerichtete automatisierte Geschäftsprozesskontrollen gewährleistet. Berichte über kritische Berechtigungen und Berechtigungskonflikte werden in automatisierter Form erstellt.



# Censys

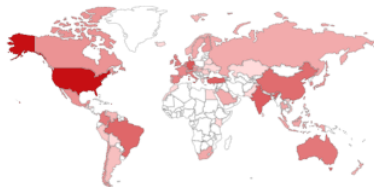


# SHODAN

## TOTAL RESULTS

2,314

## TOP COUNTRIES



United States	740
Germany	166
India	142
Turkey	130
Brazil	111

## TOP SERVICES

HTTPS	1,652
HTTP	312
HTTPS (8443)	62
HTTP (8080)	24
Qconn	22

## TOP ORGANIZATIONS

Honeywell International	36
Amazon.com	36
Microsoft Azure	33
Vodafone Net Iletisim Hizmetleri An...	31
Flycom Comunicaciones	16

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

## SAP NetWeaver Application Server Java

Mexico, Guadalajara  
Technologies:

### SSL Certificate

Issued By:  
|- Common Name: DigiCert SHA2 Secure Server CA  
|- Organization: DigiCert Inc  
Issued To:  
|- Common Name:  
|- Organization:  
S.A. DE C.V.

### Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 200 OK

server: **SAP** NetWeaver Application Server 7.22 / AS **Java** 7.11  
content-type: text/html  
last-modified: Sun, 15 Jan 2012  
cache-control: max-age=604800  
**sap**-cache-control: +86400  
**sap**-isc-etag: J2EE//  
content-length: 8527  
date: Sun, 22 Sep 2019 15:24:37 GMT

Germany

### SSL Certificate

Issued By:  
|- Common Name: GlobalSign Domain Validation CA - SHA256 - G2  
|- Organization:  
Issued To:  
|- Common Name:  
gaspici1p.sap.gascade.de

### Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

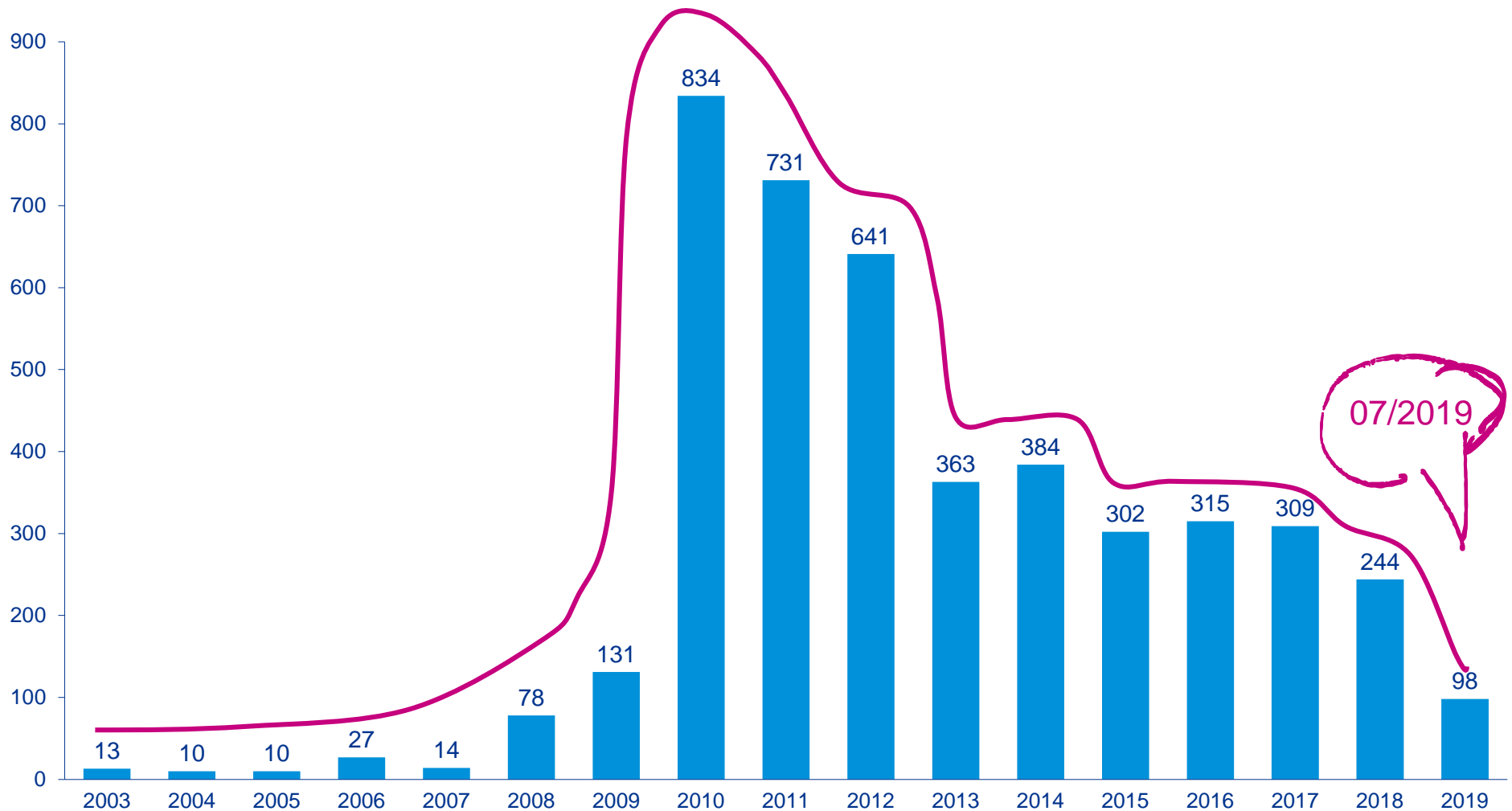
### Diffie-Hellman Parameters

Fingerprint: RFC3526  
16

HTTP/1.1 302 Found

Date: Sun, 22 Sep 2019 14:55:37 GMT  
Server: **SAP** NetWeaver Application Server 7.53 / AS **Java** 7.40  
location:  
Strict-Transport-Security: max-age=1  
Transfer-Encoding: chunked



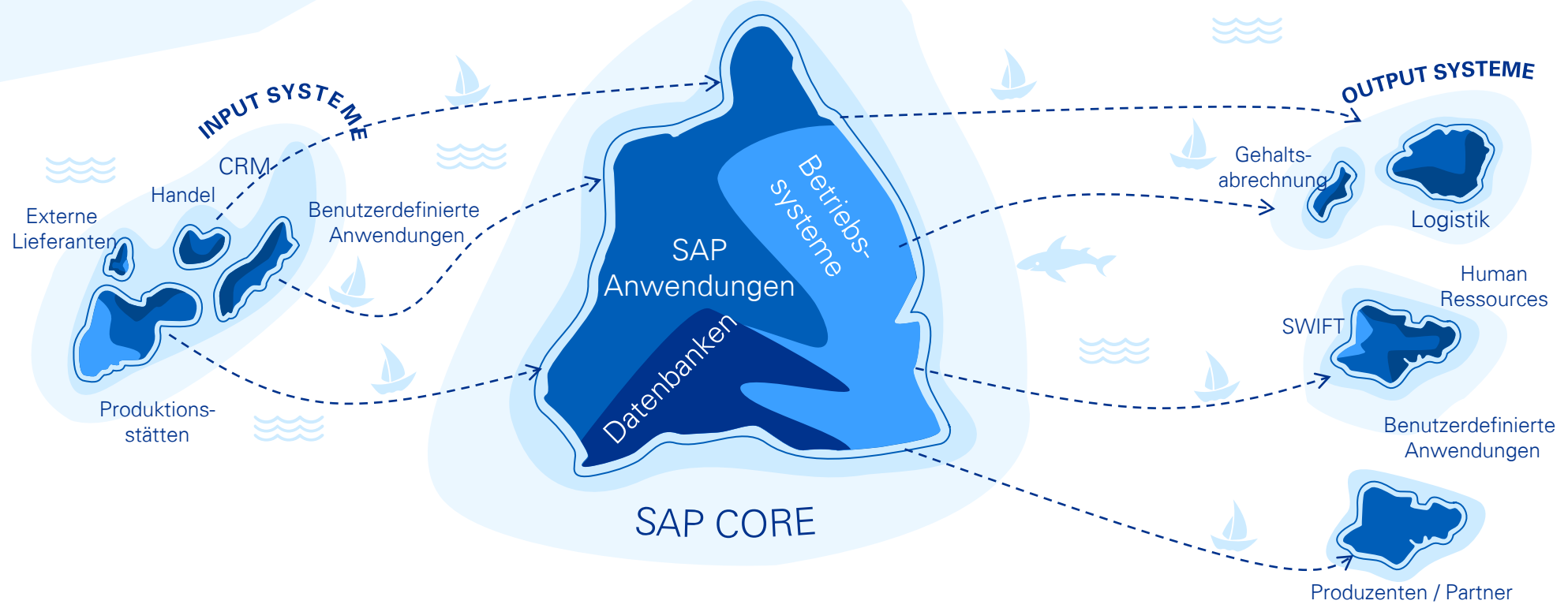


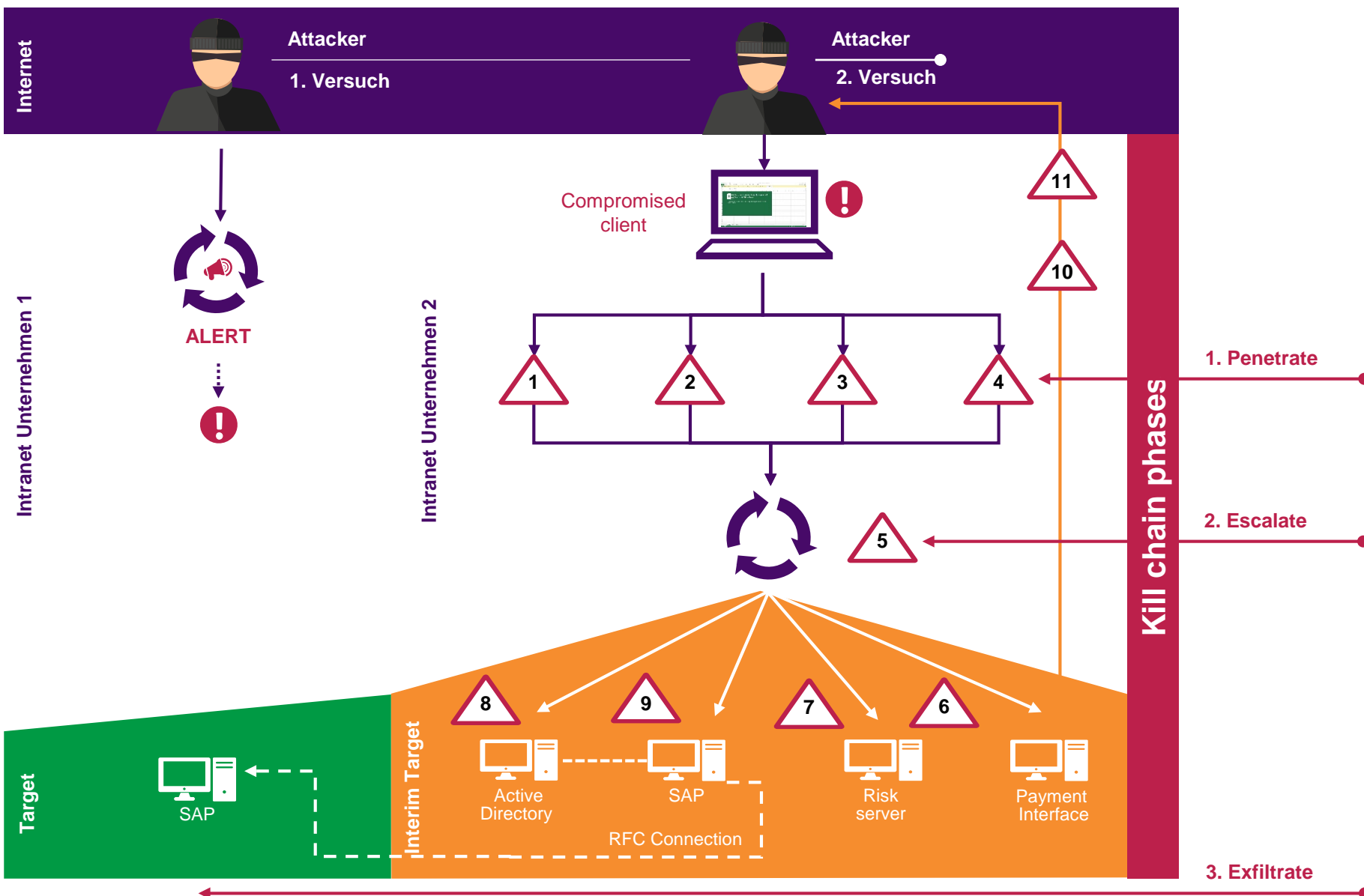
Quelle: SAP Security Notes Per Year – sap.com



# Der Angriff

Unterschiedliche Wege zum Ziel








# How a fish tank helped hack a casino

By **Alex Schiffer**

July 21, 2017

Hackers are constantly looking for new ways to access people's data. Most recently, the way was as simple as a fish tank.

-  **Industry:** Gaming and entertainment
-  **Point of Entry:** Connected fish tank
-  **Apparent Objective:** Take control of an IoT device to steal valuable information



Quelle: <https://reefbuilders.com/2017/08/07/aquarium-controller-used-to-hack-casino/>

Untypische  
Verbindungsart

Ungewöhnliche  
Datenmenge

Ungewöhnliches  
Ziel

IT-SICHERHEIT

## Hacker: Hatten Zugriff auf Steuerung von Tiroler Gondelbahn

Sicherheitsforscher entdecken gravierende Sicherheitslücken bei Patscherkofel-Anlage, Betreiber beschwichtigt

20. April 2018, 08:17 83 Postings

## Cyberattacke gegen Meier Tobler legt Betrieb weitgehend lahm

Ein Cyberangriff hat diese Woche den Schweizer Haustechnik-Spezialisten Meier Tobler lahm gelegt.

meier  
tobler

Cyberangriff auf Meier Tobler

Beim Haustechnik-Anbieter **Meier Tobler** hat ein Angriff auf die IT-Infrastruktur den Betrieb weitgehend blockiert. Wie aus einer Mitteilung des an der Schweizer Börse kotierten Unternehmens hervorgeht, sind von der Cyberattacke das zentrale Warenbewirtschaftungssystem, das Lagerleitsystem, die Festnetztelefonie, die Webseite sowie alle Email-Konten betroffen.

## Cyberattacke bei Liftkomponentenfirma Wittur

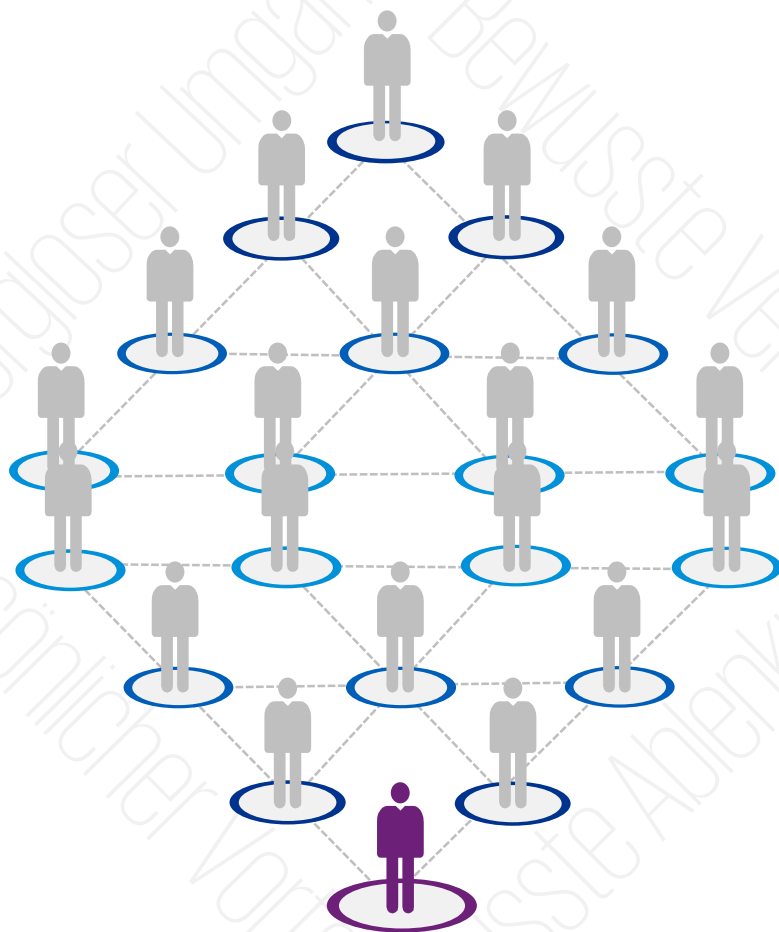
Die deutsche Firma Wittur, die Komponenten für Aufzüge herstellt und ein Werk in Scheibbs betreibt, ist Opfer einer Cyberattacke geworden. Die Fertigung stand weltweit still. Diverse Server mussten heruntergefahren werden.





# Die Aufarbeitung

Reaktion beim Ziel und ein Blick über den Tellerrand hinaus



# Third Party-Risiko...und Pflichten?



Quelle: KPMG Cyber Security Studie 2019 <https://www.kpmg.at/cyber>



Am Ende liegt es an den Mitarbeitern,...  
...ob Angreifer erfolgreich sind oder nicht!



# Ihre Ansprechpartner



**Mag. (FH) Susanne Flöckner**  
**CIA, CFE, Quality Assessor IIA**

**Partnerin Forensic & Compliance**

KPMG Advisory GmbH  
Porzellangasse 51  
1090 Wien

T +43 1 31 332-3816  
M +43 664 816 12 57  
sfloeckner@kpmg.at  
kpmg.at



**DI Robert Lamprecht, MSc**  
**CISA, CISM, CPTS, ITSM**

**Director Cyber Security, IT-Advisory**

KPMG Advisory GmbH  
Porzellangasse 51  
1090 Wien

T +43 1 31 332-3409  
M +43 664 816 12 32  
rlamprecht@kpmg.at  
kpmg.at





**kpmg.at**

© 2019 KPMG Advisory GmbH, Austrian member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative („KPMG International“), a Swiss entity. All rights reserved. Printed in Austria. KPMG and the KPMG logo are registered trademarks of KPMG International.