Security Incident Handling ex post

FG SECMGT | Gesellschaft für Informatik e. V.

Mit gerade mal vier Jahren sind wir ein noch sehr junges Zahlverfahren und haben schon viel erreicht.

rund 2,8 Mio.
Kunden (Mitte 2019)

haben sich bereits für paydirekt registriert.

mit rund 1.400
Banken und Sparkassen

bieten nahezu alle deutschen Banken und Sparkassen paydirekt an.

in über 10.000
Online-Shops

kann bereits mit paydirekt bezahlt werden. Auch in über 500 Kommunen ist paydirekt live oder im Onboarding.

rund 50%
Marktanteil

unter den EHI-Top-20-Online Shops – darunter OTTO, notebooksbilliger.de, Deutsche Bahn, bonprix, MediaMarkt, Alternate, Saturn, Schalke04, Doc Morris und BAUR.

UNTERNEHMENSINFO

Teilnehmerbanken (Auswahl)

UNTERNEHMENSINFO

Unsere Referenzen (Auswahl)

STANDORTBESTIMMUNG

„…Nach dem Knall“

Bildquellen: stockata.de

UMFRAGE ZUR CYBERSICHERHEIT BEI 1.039 UNTERNEHMEN 2018

Status Quo

Informationssicherheit in Unternehmen…

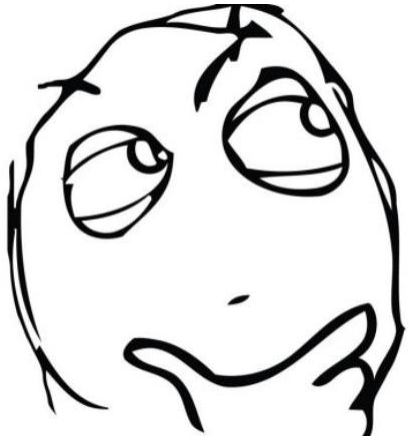
- 33% der Unternehmen hatten einen oder mehr Sicherheitsvorfälle
- 53% verfügen über kein ISMS

Auswirkungen der Sicherheitsvorfälle…

- 87% „Betriebsstörungen oder –ausfällen“
- 65% „Finanzielle Schäden“ (für Wiederherstellung)
- 22% „Reputationsschäden“

Quelle: Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2019

Hat IT-Sicherheit also für jedes dritte Unternehmen im Jahr 2019 eine hohe Priorität?



stockata.de

FALLBEISPIEL

REEDEREI A.P. MØLLER- MAERSK

- besitzt/betreibt 800 Containerschiffe und 76 Seehäfen weltweit
- befördert „20% des Welthandels“
- Sicherheitsvorfall durch die Ransomware „NotPetya“ im Juni 2017
- NotPetya verschlüsselte (fast) alle Daten (inkl. Backup)
- Mindestens 10 Tage „Downtime“
- Finanzieller Schaden zwischen 250 und 300 Mio. USD

paydirekt

FALLBEISPIEL

„NotPetya“-Angriff auf MAERSK

Quelle: www.maersk.com, 19.11.2019

flicker.com

FALLBEISPIEL

MAERSK | Weltwirtschaftsforum 2018

- *“we were basically average when it comes to cybersecurity, like many companies, and this was a wake up call”*
- *“we chose a very open dialogue around this from day one.”*
- *“it is time to stop being naive when it comes to cybersecurity”*
- *“it is very important that we are not just reactive but proactive”*
- *“We can't be average. We got to be the best we can.”*

Jim Hageman Snabe, Chairman of the Board auf dem Weltwirtschaftsforum 2018

stockata.de

FALLBEISPIEL

Follow-Up MAERSK

- *“It will also be a priority to strengthen the IT backbone and increase cyber resilience.”*

Quelle: 2017 Annual Report, A.P. Møller-Maersk A/S

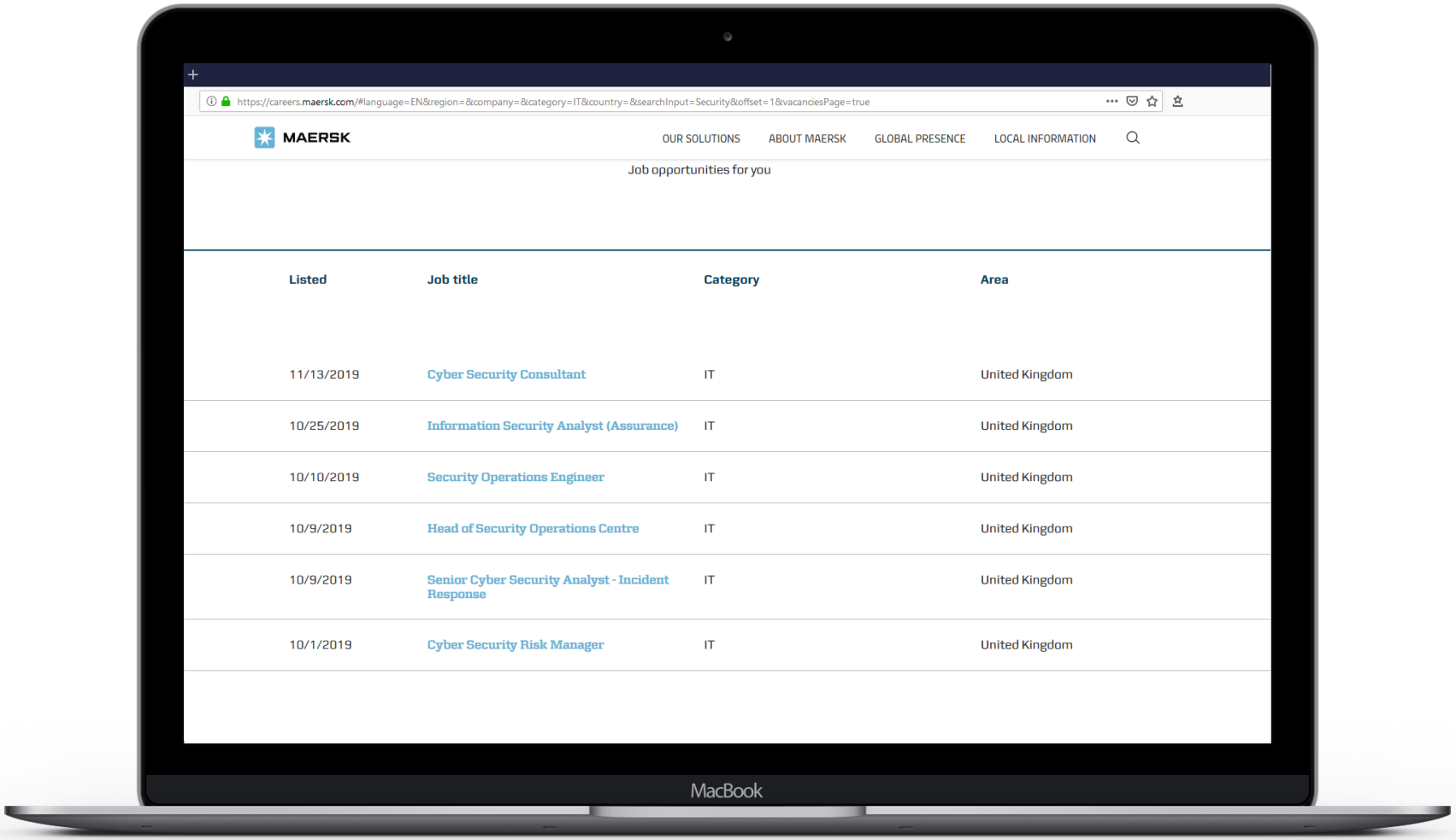
- *“It is a strategic priority to continue to improve cyber security through the cyber security plan that was launched after the cyber-attack in 2017.”*
- *“Adoption and monitoring of a new IT strategy and cyber security standard.”*
- *“Assist in setting the standard and ambition level for the IT strategy and cyber security and follow-up on progress.“*

Quelle: 2018 Annual Report, A.P. Møller-Maersk A/S

paydirekt

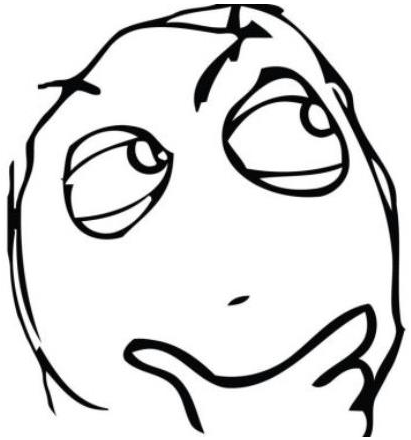
FALLBEISPIEL

MAERSK: Investitionen in Informationssicherheit



Quelle: www.maersk.com, 19.11.2019

Was können wir von diesem Fallbeispiel lernen?



Ein (schwerwiegender) Sicherheitsvorfall setzt Ihren ISMS-Prozess zurück.

Arbeiten Sie den Vorfall zeitnah und möglichst vollständig auf und lassen Sie ihr Unternehmen daraus lernen…

paydirekt

stockata.de

GRUNDLAGEN

Basisanforderungen an ein ISMS

- Klare Verantwortlichkeiten
- Sponsor im Top Management / Akzeptanz bei den Führungskräften
- Plan/Strategie
- Budget und Ressourcen
- Offensive Kommunikation nach innen und außen

VERANTWORTLICHKEITEN

Definieren Sie eindeutige Verantwortlichkeiten

- Wer ist für Informationssicherheit zuständig?
- Wie groß ist der risk appetite des Top Managements?
- Wer definiert einen „Sicherheitsvorfall“ bei Ihnen? Passt diese Definition noch?
- Wer ist verantwortlich für die Bearbeitung und ggf. Akzeptanz von ISMS-Risiken?
- Wie lange dürfen ISMS-Risiken im Unternehmen „schlummern“?
- Wie soll damit umgegangen werden, wenn ISMS-Risiken nicht bearbeitet werden?

PLAN/STRATEGIE

Agieren Sie planvoll und vereinbaren Sie Ressourcen

- Erstellen Sie eine kurzfristige, mittelfristige und langfristige Planung
- Evaluieren Sie die vorhandenen Konzepte und Regelungen sorgfältig
- Erstellen Sie eine Budgetplanung zur Verbesserung des ISMS
- Binden Sie externe Experten zur Analyse vorhandener Prozesse und Systeme ein
- Sensibilisieren Sie Führungskräfte und Mitarbeiter

KOMMUNIKATION

Kommunizieren Sie offen und in alle Richtungen

- Vereinbaren Sie regelmäßige Termine mit dem Top Management, um diese über den Zustand des ISMS und den Stand der Maßnahmenplanung zu informieren
- Die Kollegen für Informationssicherheit sensibilisieren ist weit mehr als nur ein Webinar
- Kennen Sie eigentlich die CISOs ihrer wichtigsten Dienstleister, Kunden, Anteilseigner oder auch Wettbewerber?
- Sprechen Sie mit Ihrer Marketing-Abteilung: In Social Media über Informationssicherheit sprechen, muss kein „No Go“ sein
- Wie danken Sie es eigentlich Ihren Kollegen, wenn diese Sie auf Schwachstellen hinweisen?

stockata.de

KURZFRIST-MAßNAHMEN-PLANUNG

3 Monate

- Beheben der Schwachstelle
- Erstellen und Beschluss der Budget-Planung
- Prüfung des Security Incident Handling-Prozesses
- Prüfung des IT-Forensik-Prozesses
- Einbindung von externen Experten
- Start der internen Sensibilisierung und Kommunikation

paydirekt

MITTELFRIST-MAßNAHMEN-PLANUNG

3 bis 12 Monate

- Überprüfen des „ISMS-Scopes“ bzgl. Reichweite und Wirksamkeit
- Evaluation und Erweiterung der internen Konzepte
- Aufbau eines „Gleichgesinnten“-Netzwerks mit anderen IT-Sicherheitsverantwortlichen
- Auskehr interner ISMS-Risiken
- Sensibilisierung der Mitarbeiter
- Planung und Beginn der Umsetzung kleinerer technischer Maßnahmen

LANGFRIST-MAßNAHMEN-PLANUNG

12 bis 36 Monate

- Umsetzung technischer und infrastruktureller Maßnahmen
- Anpassung von Verträgen und SLAs
- Durchführung interner Audits
- Internes „Bug Bounty“-Programm
- Überprüfen und Aktualisieren der internen Budget- und Ressourcenplanung
- Aufrechterhaltung der Sensibilität
- Ggf. Aufbau interner personeller Ressourcen

DANKE FÜR IHRE ZEIT!

Welche Fragen haben Sie?

Christopher Ruppricht
Chief Information Security Officer

Phone +49 (0) 69 247 5382 - 335
christopher.ruppricht@paydirekt.de

INFORMATIONEN ZUR DOKUMENTENWEITERGABE

Klassifikation der Folien gemäß des „Traffic Light Protocol (TLP)“*

Klassifikation	Definition
TLP: WHITE	Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe „TLP: WHITE“ ohne Einschränkungen weitergegeben werden.
TLP: GREEN	Informationen in dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Information darf jedoch nicht veröffentlicht werden.
TLP: AMBER	Informationen in der Stufe „TLP: AMBER“ dürfen innerhalb der Organisationen der Empfänger weitergegeben werden, wenn dies zur Erledigung der Tätigkeiten zwingend erforderlich ist („Need-to-know“).
TLP: RED	Informationen der Stufe „TLP: RED“ sind auf den Kreis der Anwesenden in einer Besprechung oder in einer Video-, Web- oder Telefonkonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Die Weitergabe ist durch den Ersteller untersagt.