Digitalisierung 4.0 – Chancen und Risiken für die Wirtschaft

Club Tirol, 06 10 2020

bpn-group.com

AGENDA

01 **Wie wird tatsächlich angegriffen?**

02 **Wie abwehrbereit sind wir?**

03 **Wie können wir uns besser schützen?**

CHINA UNTER VERDACHT

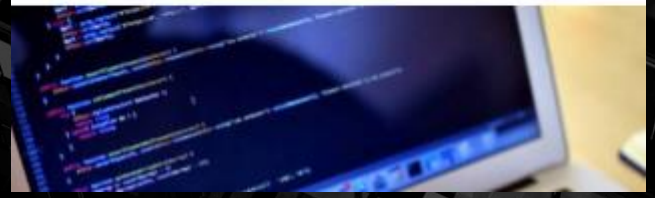
Australien beklagt schwere „staatsbasierte“ Cyberattacke

Von Till Fähnders
Veröffentlicht am 19.06.2020 - 06:34

KAMPF UM BEWERBER

Unternehmen finden nur schwer IT-Fachkräfte

Veröffentlicht am 21.09.2020 - 13:47



GRUPPE AUS KREML-UMFELD

Russische Hacker greifen Coro-na-Forscher an

Von Jochen Buchsteiner
Aktualisiert am 16.07.2020 - 19:22

CYBERATTACKE AUF BUNDESTAG

Russische Hacker sollen Mails von Kanzlerin Merkel erbeutet haben

Veröffentlicht am 08.05.2020 - 11:42

golem.de
IT-NEWS FÜR PROFIS

ÖSTERREICH

Hackerangriff bei A1 Telekom

Der größte Telefonanbieter in Österreich war über mehrere Monate Opfer eines Hackerangriffs. Aufgedeckt wurde das durch einen anonymen Whistleblower.

9. Juni 2020, 14:44 Uhr, Hanno Böck

SMS-Nachricht
Heute, 15:19

Hallo, Ihr Paket: [redacted], wurde wegen fehlenden Portos bei DHL in Peggau zurückgehalten. Bestätigen Sie hier: http://isn.dog/K7O5Z59

IT-Security informiert aus aktuellem Anlass

Dank einer aufmerksamen Mitarbeiterin konnte ein versuchter Angriff vereitelt werden, bei dem erstmals vor dem Versand der Mail mit schadhaftem Anhang ("Trojan.OLE2.Vbs-heuristic.druvzi"), von einer offiziellen [redacted] Nummer ([redacted]) angerufen wurde. In diesem Telefonat wurde darum gebeten den Anhang zur vermeintlich offenen Zahlung zu öffnen und die Makros, welche per Default aufgrund unserer Sicherheitsrichtlinie deaktiviert sind, zu aktivieren. In diesem Fall würde dieser Trojaner, eine schadhafte Software aus dem Netz laden.
Erkenntlich wurde der Angriff einerseits durch den doch eher ruppigen Ton am Telefon, sowie der Mailadresse [redacted]eu, statt der eigentlichen offiziellen [redacted]com. Die Firma [redacted]wurde informiert, als weitere Sofortmaßnahme sperrt die IT die genannte Domain [redacted]eu.
Wir bitten dennoch um erhöhte Vorsicht und Sensibilität gegenüber verdächtigen Anrufen und vermeintlich schadhaften Spammails mit Anhängen. Im Zweifelsfall wenden Sie sich bitte an den IT-Helpdesk (DW [redacted]).
Vielen Dank!

What ill do:
Ill do anything for money, im not a pussy :) if you want me to destroy some bussiness or a persons life, ill do it!
Some examples:
Simply hacking something technically
Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.
Economic espionage
Getting private information from someone
Ruining your opponents, bussiness or private persons you dont like, i can ruin them financially and or get them arrested, whatever you like.
If you want someone to get known as a child porn user, no problem.

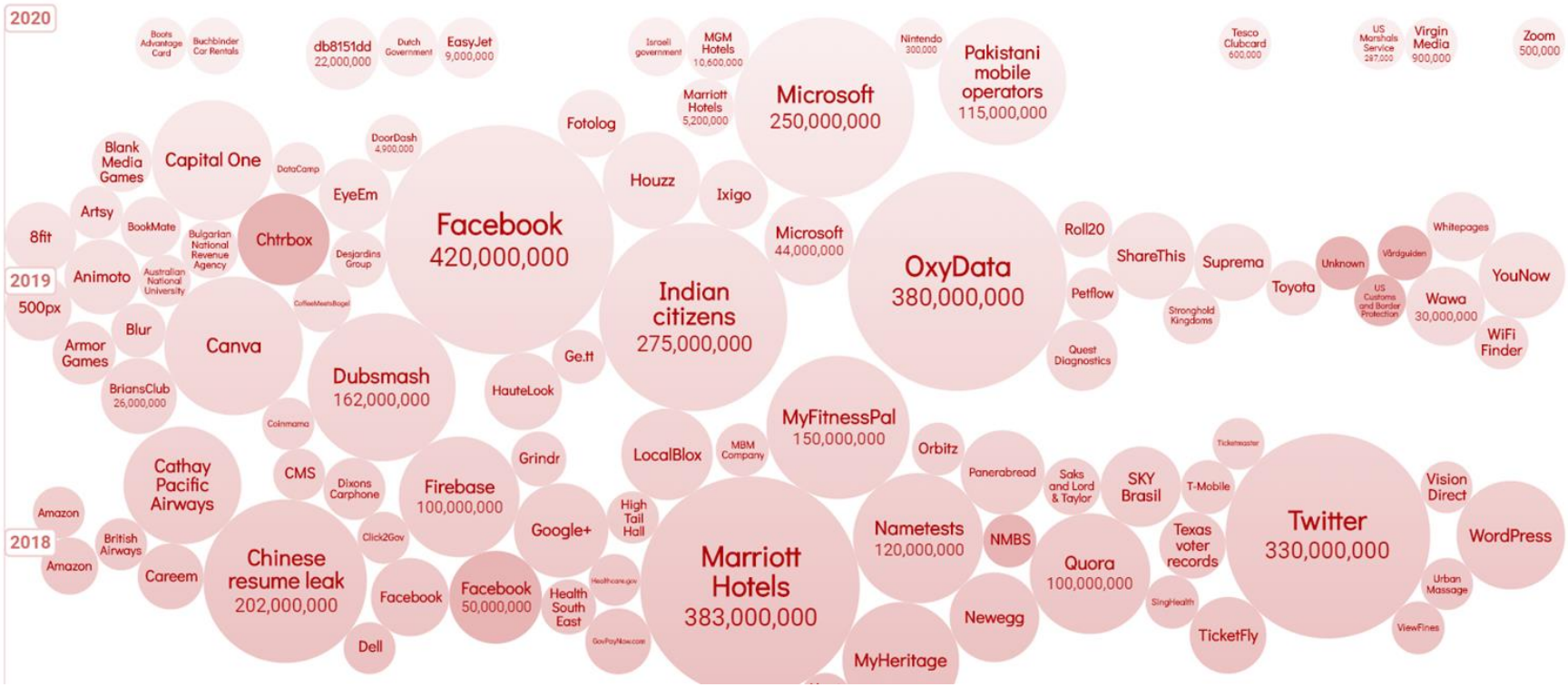
WIE WIRD TATSÄCHLICH ANGEGRIFFEN?

Bedrohungslandschaft Cyberkriminalität, Wirtschafts- und Industriespionage

https://cybermap.kaspersky.com/#

WIE WIRD TATSÄCHLICH ANGEGRIFFEN?

Bedrohungslandschaft Cyberkriminalität, Wirtschafts- und Industriespionage



https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

WIE ABWEHRBEREIT SIND WIR?

Erfahrungen

"The economic implications of **cyber risk have to be quantified** into monetary value for cyber risk management to transform **from a compartmentalized technical issue into a business issue**, formally integrating it into Enterprise Risk Management (ERM) …"

"…**new digital business models** are the principal reason why just over half of the names of companies on the Fortune 500 have disappeared since the year 2000"

"…transforming Information Technology (IT) **from a supportive operational role into the business critical role** of core value creation "

„…als weltweites **Top-Risiko für Unternehmen aller Branchen** und jeder Größenordnung gelten mittlerweile Cyber-Vorfälle."

Keyun Ruan, Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomics, 2019

Pierre Nanterme (CEO of Accenture): World Economic Forum's Annual Meeting in Davos

Keyun Ruan, Introducing cybernomics: a unifying economic framework for measuring cyber risk, Computers & Security, 2016

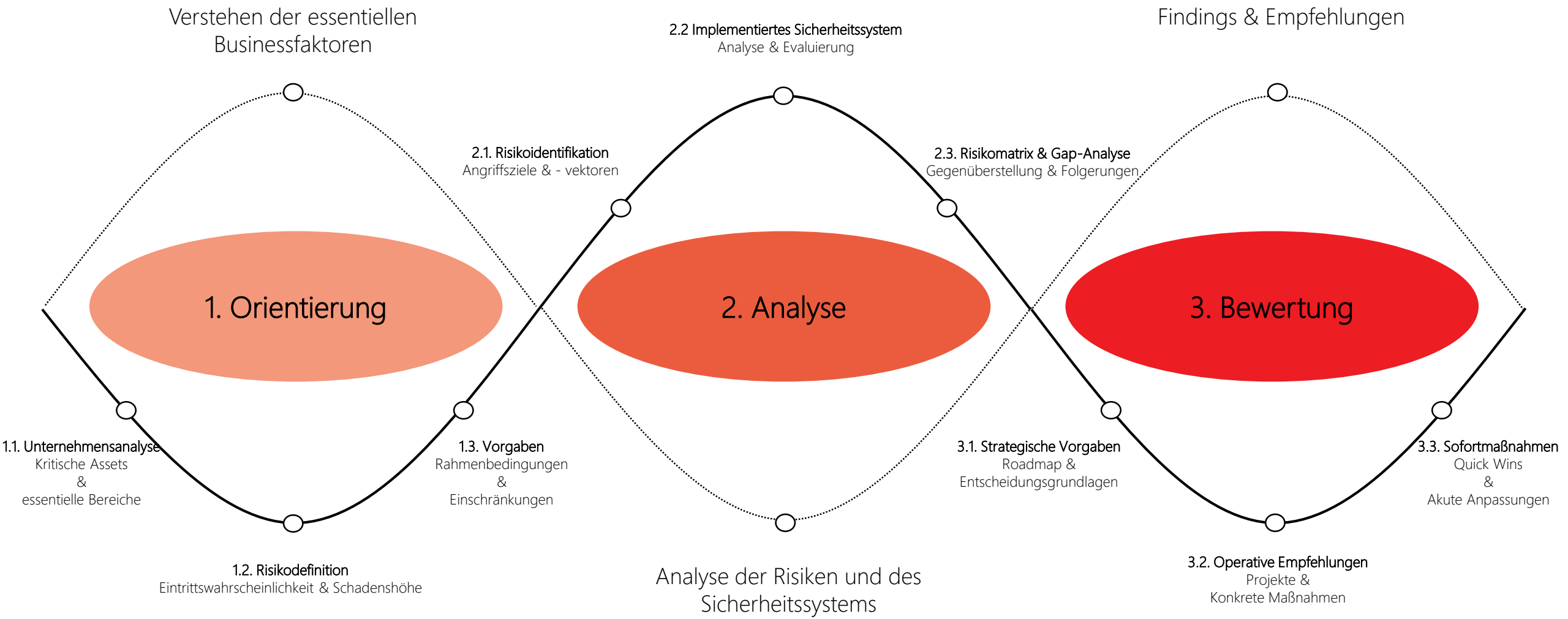
Allianz Risk Barometer 2020

WIE ABWEHRBEREIT SIND WIR?

Erfahrungen

Langjährige Angriffserfahrung großangelegter Cyber- und Spionageangriffe zeigt insbesondere:

- Die Identifikation und Bewertung **schützenswerter Bereiche (sog. Assets)** erfordert die Einbeziehung einer Vielzahl von Variablen.
- Die Einschätzung von **Risiken und konkreten Bedrohungsszenarien** ist schwierig und häufig bereits erste Fehlerquelle.
- Abwehrfähigkeit ist nur mit **ganzheitlichem** Zugang zu erreichen.
- Eine ganzheitliche Betrachtung eröffnet eine Vielzahl unterschiedlicher **Maßnahmen**, die es zu **strukturieren und umzusetzen** gilt.
- Strukturierung erforderlicher Maßnahmen (bspw. in Form von Roadmaps) und deren Umsetzung ist **keine Aufgabe für „Nebenbei“.**
- Auftretende Incidents bringen unweigerlich ans Licht, wer vorbereitet und abwehrfähig ist.


Verstehen der essentiellen Businessfaktoren
2.2 Implementiertes Sicherheitssystem
Analyse & Evaluierung
Findings & Empfehlungen
2.1. Risikoidentifikation
Angriffsziele & - vektoren
2.3. Risikomatrix & Gap-Analyse
Gegenüberstellung & Folgerungen
1. Orientierung
2. Analyse
3. Bewertung
1.1. Unternehmensanalyse
Kritische Assets
&
essentielle Bereiche
1.3. Vorgaben
Rahmenbedingungen
&
Einschränkungen
3.1. Strategische Vorgaben
Roadmap &
Entscheidungsgrundlagen
3.3. Sofortmaßnahmen
Quick Wins
&
Akute Anpassungen
1.2. Risikodefinition
Eintrittswahrscheinlichkeit & Schadenshöhe
Analyse der Risiken und des Sicherheitssystems
3.2. Operative Empfehlungen
Projekte &
Konkrete Maßnahmen


BPN
vienna@bpn-group.com
bpn-group.com