



# CYBERKRIMINALITÄT UND -SECURITY FORTGESCHRITTENE

## WICHTIGE BEGRIFFE ZU CYBERKRIMINALITÄT UND -SECURITY

### CYBERKRIMINALITÄT

Der Begriff Cyberkriminalität beschreibt kriminelle Aktivitäten, die mithilfe von digitalen Technologien ausgeführt werden.

### CYBERSECURITY

Cybersecurity verbindet technische und organisatorische Aspekte, wie z.B. Sicherheitssysteme, Prozessdefinitionen, Leitlinien, Pflichtenhefte oder auch Schulungen zur Sensibilisierung von Mitarbeitern.



## WIE KÖNNEN SICH UNTERNEHMEN SCHÜTZEN?



1. Auch kleine und mittelständische Unternehmen benötigen ein umfassendes Sicherheitspaket
2. Besonders sensible Bereiche müssen identifiziert werden, um diese vermehrt schützen zu können
3. Es ist eine umfassende Sicherheitslösung zu empfehlen, die auch Mobiltelefone einschließt
4. Alle Standards müssen eingehalten werden
5. Alle Mitarbeiter müssen geschult und für Online-Gefahren sensibilisiert werden
6. Auf eine Sicherheitslösung, die Systeme und Netze in Echtzeit überwacht ist zu favorisieren

## WIE WIRD BEI EINER CYBERATTACKES RICHTIG KOMMUNIZIERT?

- Für interne Kommunikation benötigen die Fachabteilungen natürlich die für sie relevanten Informationen.
- Für externe Kommunikation ist es für die Kunden wichtig zu wissen, ob sie z.B. ihre Kreditkarte sperren lassen müssen. Außerdem kann man bei frühzeitiger Kommunikation auf die Toleranz der Betroffenen hoffen und so den Imageschaden minimieren.



## WUSSTEST DU SCHON?

Im Darknet wird mit sogenannten Kryptowährungen wie z.B. Bitcoin oder Ether bezahlt, um die Anonymität zu wahren.\*

\*<http://t3n.de/news/bitcoin-ether-kryptowaehrung-802230/>

## WAS IST VOR EINER CYBERATTACKES ZU KLÄREN?

Um bei einer Cyberattacke schnell und richtig handeln zu können, müssen folgende Dinge vorab geklärt werden:

### **BUSINESS CONTINUITY**

- Welchen Einfluss hat der Ausfall von bestimmten Systemen auf das Tagesgeschäft?
- Um bei einem Angriff weiterhin dem Kundengeschäft nachgehen zu können, sollten Firmen für sehr wichtige Systeme über den ganzen Globus verteilte Datacenter mit den exakt gleichen Daten haben. So stehen diese Daten im Notfall weiterhin zur Verfügung.

### **INCIDENT RESPONSE**

- Welchen Plan verfolgen wir, wenn eine Cyberattacke stattfindet?
- Dafür sollte man z.B. erfahrene und vertrauenswürdige Experten einbinden, die das Unternehmen dabei unterstützen, die richtigen Maßnahmen zu finden. Damit die Experten schlimmeres verhindern und unverzüglich mit der Arbeit beginnen können, müssen ihnen die technischen und finanziellen Ressourcen unverzüglich zur Verfügung gestellt werden.