BREDEX

# Spionage vs. Ransomware

## Geschäftsgeheimnisse als Ziel von Hackern

# ~$whoami

Kevin Keller
Informationssicherheitsberater Bredex GmbH
Zert. BSI Grundschutzpraktiker
Zert. Automotive Cybersecurity Engineer (ISO/SAE 21434)
TISAX Beratung
CTF / Web-Penetration-Testing

# Agenda

1. Einführung in das Thema
2. Auswirkungen der Produktpiraterie auf die Unternehmen
3. Schutz vor Produktpiraterie
4. Wirtschaftsspionage / Ransomware
5. Informationsklassifizierung und weitere Schutzmaßnahmen
6. Fazit

# Einführung in das Thema

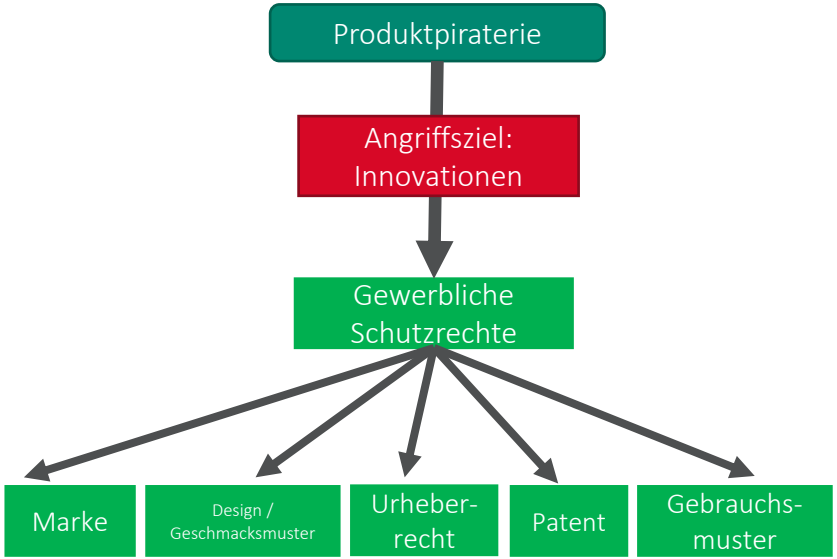
## Schäden steigen auf 223 Mrd. Euro: Erpressung und Systemausfälle als treibende Faktoren (+358% ggü. 2019)

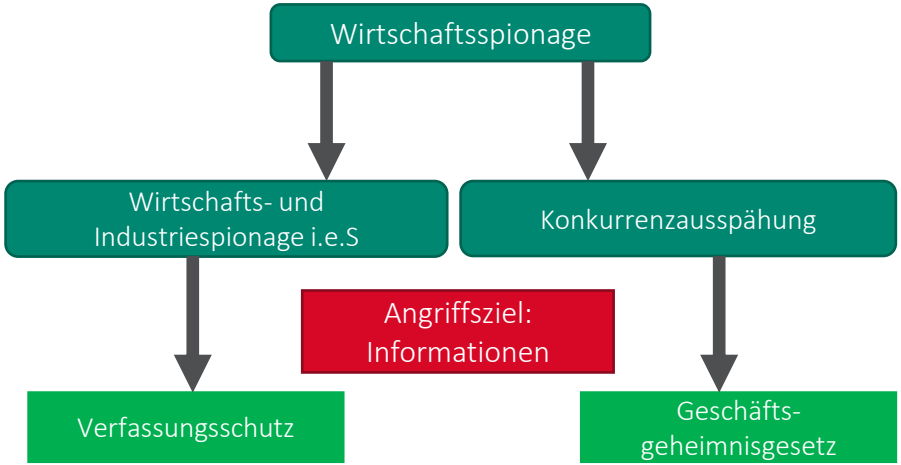
Wodurch sind Ihrem Unternehmen innerhalb der letzten 12 Monate Schäden im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

| Schaden durch... | Schadenssummen in Mrd. Euro (2021) | Schadenssummen in Mrd. Euro (2019) | Schadenssummen in Mrd. Euro (2017) | Schadenssummen in Mrd. Euro (2015) |
|---|---|---|---|---|
| Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen | **61,9** | 13,5 | 5,3 | 7,2 |
| Erpressung mit gestohlenen Daten oder verschlüsselten Daten | **24,3** | 5,3 | 0,7 | 1,5 |
| Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden) | **17,1** | 4,4 | 3,2 | 2,0 |
| Patentrechtsverletzungen (auch schon vor der Anmeldung) | **30,5** | 14,3 | 7,7 | 9,4 |
| Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen | **29,0** | 11,1 | 8,6 | 6,4 |
| Umsatzeinbußen durch nachgemachte Produkte (Plagiate) | **22,7** | 11,1 | 3,5 | 11,5 |
| Imageschaden bei Kunden oder Lieferanten/Negative Medien-berichterstattung | 12,3 | 9,3 | 7,7 | 5,9 |
| Kosten für Ermittlungen und Ersatzmaßnahmen | 13,3 | 18,3 | 10,6 | - |
| Kosten für Rechtsstreitigkeiten | 12,4 | 15,6 | 5,5 | 6,5 |
| Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern | - | - | 2,2 | 0,9 |
| Sonstige Schäden | 0 | <0,1 | <0,1 | 0,1 |
| **Gesamtschaden pro Jahr** | **223,5** | **102,9** | **54,8** | **51,2** |

Basis: Selbsteinschätzung aller befragten Unternehmen, die in den letzten 12 Monaten (vor 2021: in den letzten 2 Jahren) von Diebstahl, Industriespionage oder Sabotage betroffen waren (2021: n=935; 2019: n=801; 2017: n=571; 2015: n=550) | Quelle: Bitkom Research 2021

# Einführung in das Thema



# Einführung in das Thema

## Produktpiraterie (Plagiat / unzulässiger Nachbau)

Unter dem unzulässigen Nachbau (hier gleichbedeutend als Produktpiraterie bzw. Plagiat bezeichnet) wird der

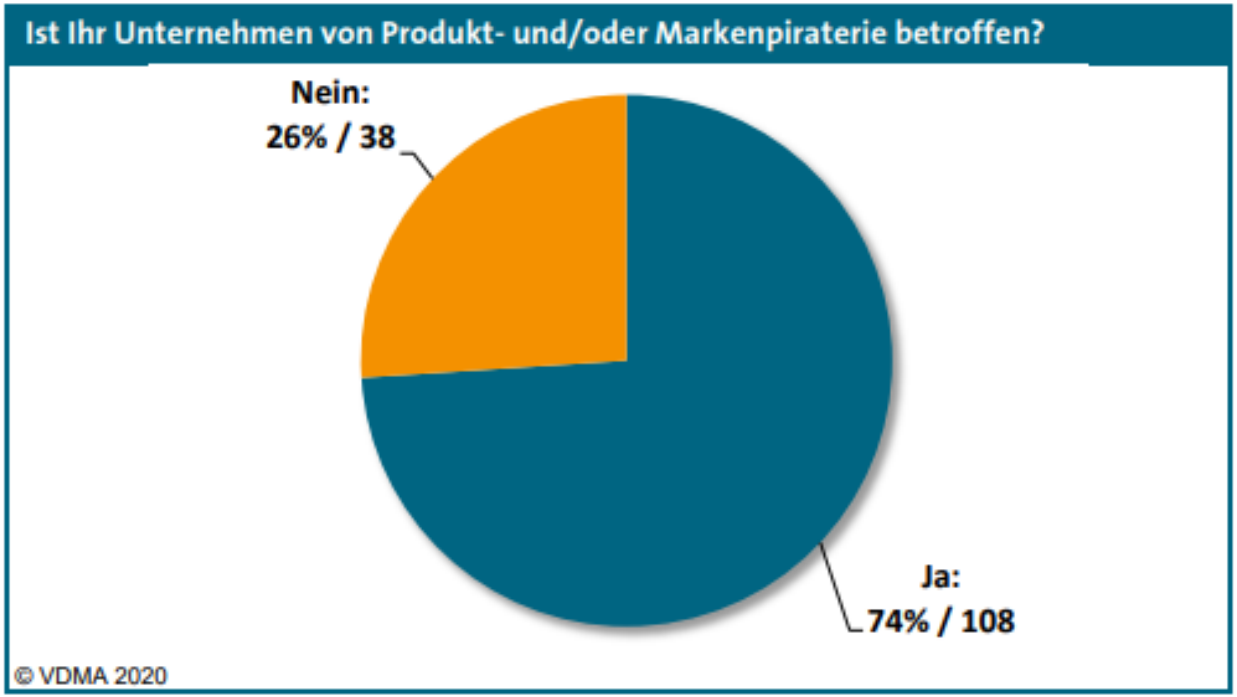
- Nachbau unter Verletzung von Sonderschutzrechten (z. B. Marken, Patente) oder
- ohne Verletzung von Sonderschutzrechten, aber in wettbewerbswidriger Weise erfolgte Nachbau verstanden.

Der Nachbau erfolgt dann in wettbewerbswidriger Weise, wenn neben der Nachahmung zusätzlich noch eine unlautere Handlung eintritt. Diese unlautere Handlung ist in der Regel eine Täuschung über den Hersteller der Originalware (Verwechslungsgefahr) und die damit verbundene Ausnutzung des guten Rufs.

# Agenda

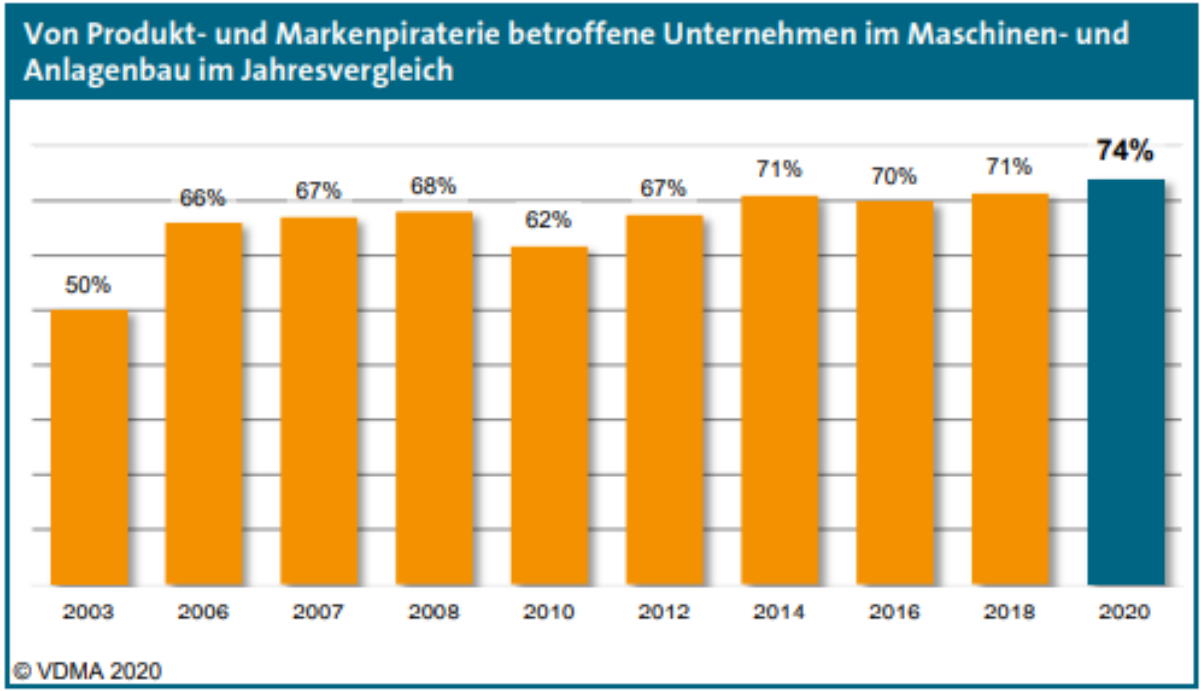
1. Einführung in das Thema
2. Auswirkungen der Produktpiraterie auf die Unternehmen
3. Schutz vor Produktpiraterie
4. Wirtschaftsspionage / Ransomware
5. Informationsklassifizierung und weitere Schutzmaßnahmen
6. Fazit

# Betroffenheit der Unternehmen




Quelle: VDMA Studie Produktpiraterie 2020 VDMA Studie Produktpiraterie

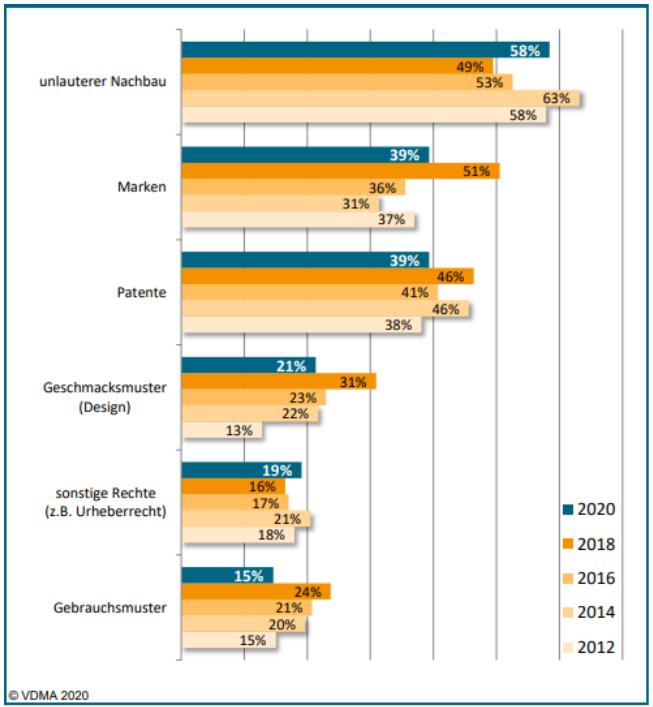
# Auswirkungen der Produktpiraterie auf die Unternehmen



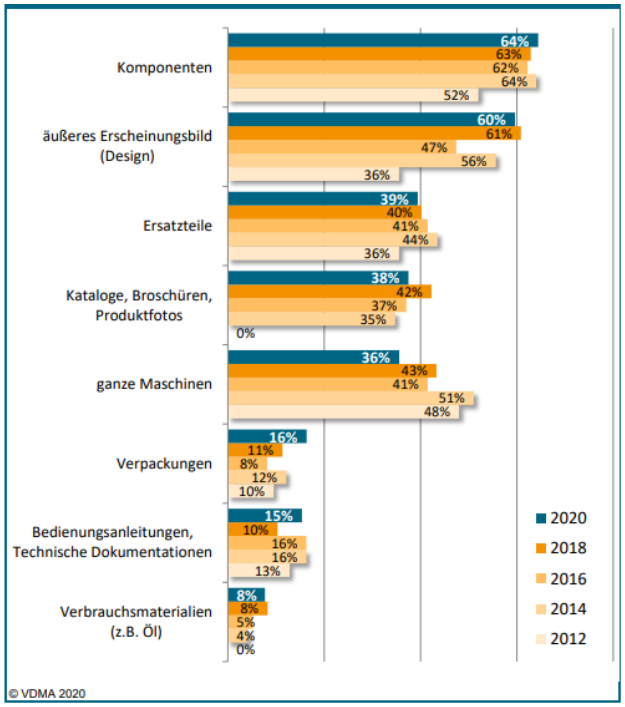

Quelle: VDMA Studie Produktpiraterie 2020 VDMA Studie Produktpiraterie

# Auswirkungen der Produktpiraterie auf die Unternehmen

Wie?




Was?




Quelle: VDMA Studie Produktpiraterie 2020 VDMA Studie Produktpiraterie

# Auswirkungen der Produktpiraterie auf die Unternehmen

Hong Wu/Getty Images

# Agenda

1. Einführung in das Thema
2. Auswirkungen der Produktpiraterie auf die Unternehmen
3. Schutz vor Produktpiraterie
4. Wirtschaftsspionage / Ransomware
5. Informationsklassifizierung und weitere Schutzmaßnahmen
6. Fazit

# Gewerbliche Schutzrechte als verbreiteteste Maßnahme

Schutzmaßnahmen

## Zur Sicherung von Innovationen (Schutz vor Piraterie)

- 86% der Unternehmen greifen zur Sicherung ihrer Innovationen auf die Anmeldung gewerblicher Schutzrechte zurück
- Dazu zählen:
  - Das Markenrecht
  - Das Design / das Geschmacksmuster
  - Das Urheberrecht
  - Das Patent
  - Das Gebrauchsmuster

# Gewerbliche Schutzrechte allein reichen nicht aus

## Schutzmaßnahmen

- Nur knapp 50% aller geschädigten Unternehmen ergreifen im Fall der Fälle tatsächlich rechtliche Schritte. Warum?
  - Erfolgsaussichten
  - Langwierigkeit
  - Das „Kind ist bereits in den Brunnen gefallen“
- Und vor Allem: Wie schützen Sie Ihre Innovationen, bevor diese den Reifegrad für ein Schutzrecht erlangt haben?

➢ **Es sind Ihre Kronjuwelen! Sichern Sie die Informationen über Ihre Kronjuwelen frühzeitig und wirksam ab ! Identifizieren und klassifizieren Sie Ihre Informationen !**

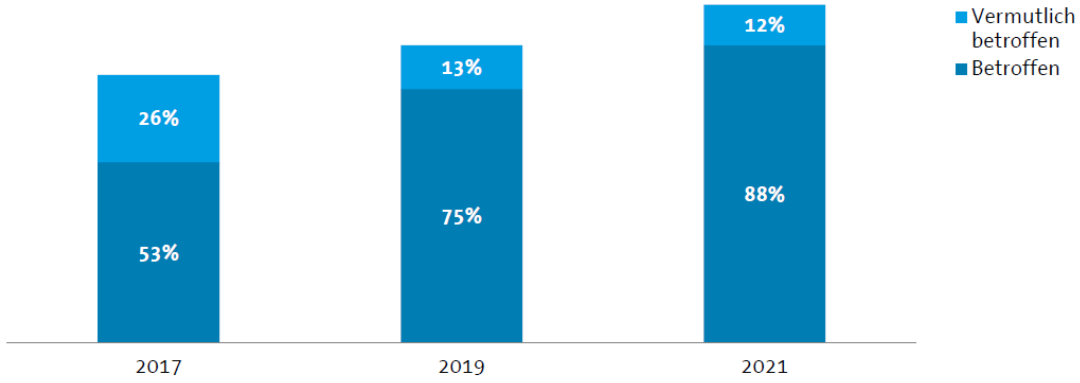
# Agenda

1. Einführung in das Thema
2. Auswirkungen der Produktpiraterie auf die Unternehmen
3. Schutz vor Produktpiraterie
4. **Wirtschaftsspionage / Ransomware**
5. Informationsklassifizierung und weitere Schutzmaßnahmen
6. Fazit

# Angriffe auf die deutsche Wirtschaft

## Deutsche Wirtschaft mehr denn je von Angriffen betroffen

War Ihr Unternehmen innerhalb der letzten 12 Monate (2017 und 2019: innerhalb der letzten zwei Jahre) von Diebstahl, Industriespionage oder Sabotage betroffen?




Basis: Alle befragten Unternehmen (2021: n=1.067; 2019: n=1.070; 2017: n=1.069); Befragungszeitraum: 11. Januar bis 09. März 2021 | Quelle: Bitkom Research 2021

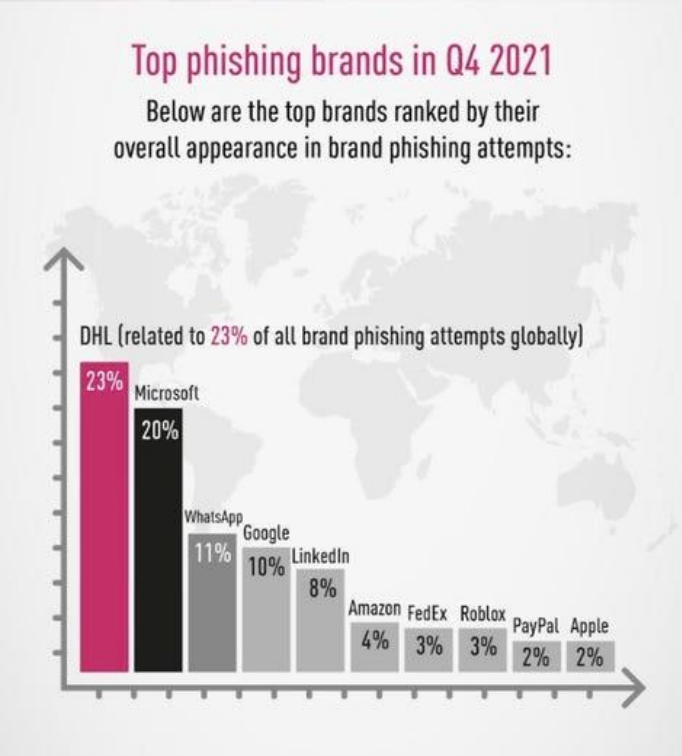
# Digitale Produktpiraterie


- The Pirate Bay

- Größter Torrent Index

- Software
- Bücher
- Filme
- Musik
- Datensätze/PII/Credentials
- Baupläne/Schemata
- Etc…

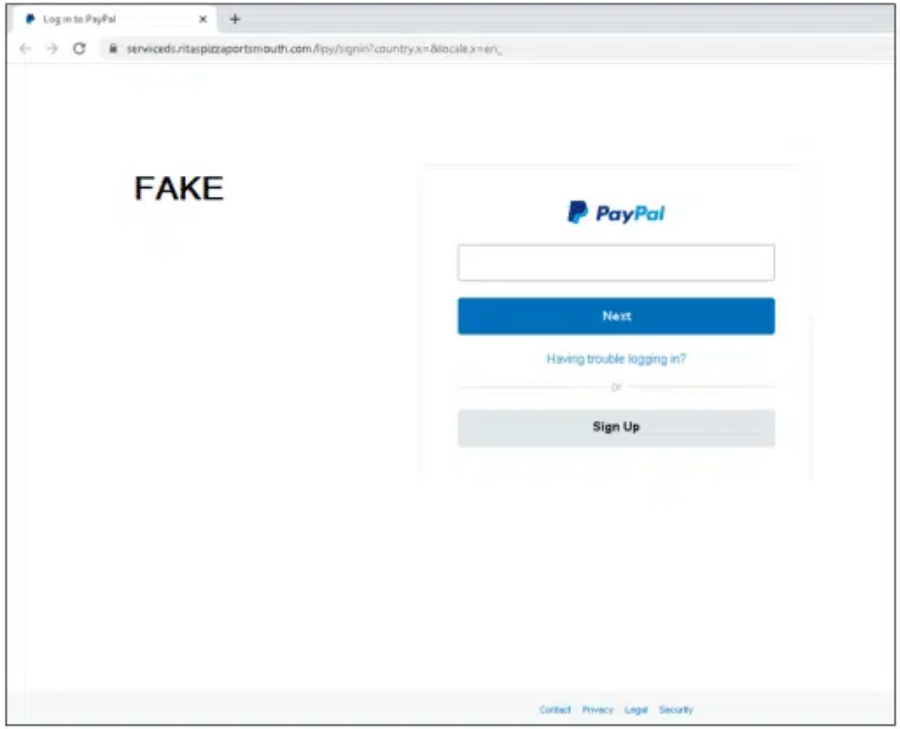
# Angriffsvektoren

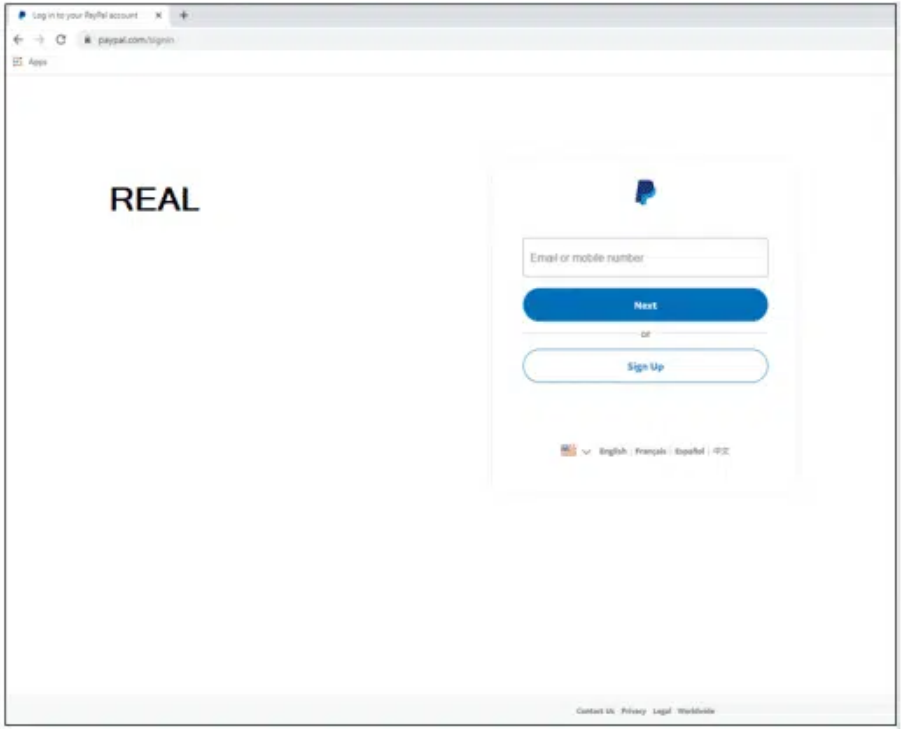



Ihr Paket wurde verschickt. Bitte überprüfen und akzeptieren Sie es. http://abcdef123dhl.org

Quelle: checkpoint.com

# Angriffsvektoren



# Ooops, your files have been encrypted!

English

Payment will be raised on

5/15/2017 16:50:06

Time Left

02:23:34:22

Your files will be lost on

5/19/2017 16:50:06

Time Left

06:23:34:22

## What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

## Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

## How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Copy

About bitcoin

How to buy bitcoins?

Contact Us

Check Payment

Decrypt

# Cyber Kill Chain


| Recon | Weaponize | Deliver | Exploit | Install | C2 | Actions |
|---|---|---|---|---|---|---|
| Gather data and intelligence on target organization | Craft malicious payload, use exploits for vulnerabilities | Payload sent to target (phishing) | Compromise system | Install malware, obtain credentials and establish backdoors. | Navigate internal network and setup command and control | Ultimate goals achieved |

# Agenda

1. Einführung in das Thema
2. Auswirkungen der Produktpiraterie auf die Unternehmen
3. Schutz vor Produktpiraterie
4. Wirtschaftsspionage / Ransomware
5. Informationsklassifizierung und weitere Schutzmaßnahmen
6. Fazit

# Mix aus betrieblichen Maßnahmen beschützt das Know-How

## Zur Sicherung des unternehmenseigenen Know-hows (Schutz vor Spionage)

- Informationssicherheit und IT-Sicherheit
- Auswahl und Schulung von Mitarbeitern
- Etablierung interner Compliance-Programme
- Sicherung von Geheimhaltung in Arbeitsverträgen
- Kontrollierte Kommunikation mit Abnehmern, Zulieferer und sonstiger Vertragspartner
- Konsequente Vereinbarung von NDAs
- Absicherung der Produktionsstandorte

# Wirtschafts- und Industriespionage i.e.S.

- Unterstützung durch Landesamt für Verfassungsschutz

- Nach Definition des Bundesamtes für Verfassungsschutz (BfV) werden die Begriffe nur dann verwendet, wenn die Spionagetätigkeit staatlich gelenkt oder gestützt wird oder fremde Nachrichtendienste die Ausforschung im Zielbereich Wirtschaft lenken.

- Liegt ein solcher Angriff vor, hilft das Landesamt für Verfassungsschutz, denn die Abwehr fremder Dienste gehört zu seinen Aufgaben (§ 3 Abs. I Nr. 2 BVerfSchG).

- In solchen Fällen kann beim zuständigen Landesamt für Verfassungsschutz um Hilfe bzw. Unterstützung gebeten werden unter: www.verfassungsschutz.de/de/landesbehoerden

# Konkurrenzausspähung

- Keine staatliche Unterstützung bei Konkurrenzausspähung
- Konkurrenzausspähung liegt vor, wenn ein fremdes oder mit einem im Wettbewerb stehendes Unternehmen die Daten ausspäht, ohne sich durch staatliche Dienste helfen zu lassen.
- Sie kommt wesentlich häufiger vor als die Wirtschafts- und Industriespionage.
- Für derartige Angriffe ist der Staat nicht zuständig. Daher muss hier jedes Unternehmen aus eigener Kraft heraus Angriffe abwehren
- ABER: Geschäftsgeheimnisgesetz

# Was ist ein Geschäftsgeheimnis?

- Inhaltliche Anforderung ist, dass dieses geheim ist
- Kein Erfordernis einer geistigen Leistung, Erfindung o.ä.
- Immer dann unverzichtbar, wenn kein Sonderrechtschutz (Patent, Marke, Urheber etc.) zur Verfügung steht bzw. die Innovation noch nicht reif für die Anmeldung eines Schutzrechts ist .
- Des Weiteren bei kurzer Laufzeit und als kostengünstige Alternative zum Schutzrecht

➢ Der Geschäftsgeheimnisschutz bildet eine sinnvolle Ergänzung des Sonderrechtsschutzes (siehe gewerbliche Schutzrechte)

# Was ist ein Geschäftsgeheimnis?

- Gemäß §2 GeschGehG:
- Ein Geschäftsgeheimnis ist eine Information……

  a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist,

  b) die Gegenstand von den Umständen nach angemessener Geheimhaltungmaßnahmen durch ihren rechtmäßigen Inhaber ist und

  c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

➢ Das bedeutet: Das Geheimnis muss „aktiv“ durch Schutzmaßnahmen geheim gehalten werden!

# Geschäftsgeheimnis

Das Geschäftsgeheimnisgesetz erfordert auch vom Unternehmen selbst entsprechende Vorkehrungen:

- Identifikation und Ergreifung von Schutzmaßnahmen
- Nach Angemessenheit und Wirksamkeit
- Dokumentation der Maßnahmen (Nachweis)

# Sicherstellung entsprechender Schutzmaßnahmen gemäß GeschGehG

- Schutzmaßnahmen lassen sich am Besten durch ein funktionierendes ISMS belegen:
  - Identifikation kritischer Informationen und Ressourcen (Schutzklassen)
  - Es gibt in Deutschland geeignete Managementstandards für KMUs

- Umgang mit sensitiven Informationen verbindlich regeln!
  - Was sind Ihre Kronjuwelen? Was sind Ihre sensitiven Informationen?
  - Nehmen Sie eine Informationsklassifizierung vor!
  - Regeln Sie den Umgang mit den Informationsklassen!

- Externe einbeziehen !
  - Vertragliche Regelungen
  - NDAs

# Ihre Mitarbeiter sollten sicher sein …

…in der Klassifizierung von Informationen:

- wie bedeutsam / kritisch ist die Mail, das Dokument, die Akte, der Ausdruck das Telefonat etc. für das Unternehmen ?

…in der Kennzeichnung der Information:

- wie werden streng vertrauliche, vertrauliche und interne Informationen gekennzeichnet?

…in der Behandlung von Informationen:

- als Ersteller / Sender
- als Empfänger

# So könnte der Umgang geregelt werden:



| Informations-klasse | Erläuterung | Beispiele | Anhaltspunkte zur Klassifizierung |
|---|---|---|---|
| S1 Öffentlich | Alle Informationen, die aus öffentlichen Quellen frei zugänglich sind bzw. öffentlich zugänglich gemacht werden können | Stelleninformationen, veröffentlichte Bilanzen, Produktinformationen, Bankleitzahl | Kein oder unwesentlicher Schaden, es ist kein Reputationsverlust zu erwarten. |
| S2 Intern | Informationen, die im Unternehmen allen Mitarbeitern zugänglich, aber nicht für Dritte bestimmt sind. | Arbeitsanweisungen / Verfahrens-beschreibungen, Organigramme | Ein Verlust der Vertraulichkeit kann zu einem geringen Schaden führen. Ein Reputationsverlust ist eher unwahrscheinlich oder tritt vereinzelt auf. |
| S3 Vertraulich | Informationen, die nur einem bestimmten internen Personenkreis bekannt sein dürfen | Personenbezogene Daten, Budgets, Auditberichte | Ein Verlust der Vertraulichkeit kann zu einem mittleren bis vereinzelt hohen Schaden führen. Eine kurzfristige Reputationswirkung ist möglich, Wettbewerbsnachteile sind nicht auszuschließen. |
| S4 Streng vertraulich | Informationen, die nur einem eng begrenzten Personenkreis bekannt sein dürfen | Betriebsgeheimnisse, besonders schützenswerte personenbezogene Daten, Strategieentscheidungen vor Veröffentlichung, Bilanzentwürfe | Ein Verlust der Vertraulichkeit könnte zu einem hohen bis sehr hohen Schaden führen z.B. durch nachhaltige Reputationswirkungen und/oder Wettbewerbsnachteile |

# So könnte der Umgang geregelt werden:



| Klasse | Zugriff | Elektr. Übertragung | Telefon | Phsyik. Übertragung | Elektr. Ablage | Physik. Ablage | Druck / Kopien | Vernichtung |
|---|---|---|---|---|---|---|---|---|
| S4 Streng vertraulich | • Interne: Nur explizit benannte Personen<br>• Externe: nein | • Intern: nur verschlüsselt<br>• extern: nur verschlüsselt | • Intern: nur n vertraulicher Umgebung<br>• Extern: generell vermeiden | • Intern: sicher verschlossen<br>• Extern: sicher verschlossen und nachverfolgbar | • Laufwerke/SharePoint: nur verschlüsselt<br>• Mobile devices: nur verschlüsselt<br>• Mobile Datenträger: nur verschlüsselt | Verschluss (Schrank oder Schreibtisch) | • Druck: direkt am Arbeitsplatz oder kennwortgeschützt<br>• Kopien: keine | • Elektr.: spez. Entsorgungsbehälter<br>• Physik.: Spez. Entsorgungsbehälter |
| S3 Vertraulich | • Interne: Explizit genannte Funktionsträger und Vertreter<br>• Externe: nur mit persönl. NDA | • Intern: unverschlüsselt<br>• extern: verschlüsselt | • Intern: nur in vertraulicher Umgebung<br>• Extern: nur in vertraulicher Umgebung | • Intern: einfach verschlossen<br>• Extern: einfach verschlossen | • Laufwerke/SharePoint: nur zugangsbeschränkte<br>• Mobile devices: nur verschlüsselt<br>• Mobile Datenträger: nur verschlüsselt | Verschluss (Schrank, Schreibtisch) | • Druck: s.o. oder sofortige Entnahme<br>• Kopien: nur wenn vorgesehen | • Elektr.: spez. Entsorgungsbehälter<br>• Physik.: Spez. Entsorgungsbehälter oder schreddern |
| S2 Intern | • Interne: Alle<br>• Externe: nur mit Geheimhaltungsvereinbarung Unternehmen | • Intern: unverschlüsselt<br>• extern: unverschlüsselt | Intern: uneingeschränkt<br>Extern: nur in vertraulicher Umgebung | • Intern: offen<br>• Extern: einfach verschlossen | • Laufwerke/SharePoint: alle<br>• Mobile devices: nur verschlüsselt<br>• Mobile Datenträger: nur verschlüsselt | Im Gebäude | • Druck: keine Einschränkung<br>• Kopien: nur innerhalb Gebäude | • Elektr.: spez. Entsorgungsbehälter<br>• Physik.: Spez. Entsorgungsbehälter oder schreddern |

# Beispiel: Konzept für Auslandsdienstreisen nach BSI


- Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen
- Sensibilisierung der Mitarbeiter zur Informationssicherheit auf Auslandsreisen
- Identifikation länderspezifischer Regelungen, Reise- und Umgebungsbedingungen
- Verwendung von Sichtschutz-Folien
- Verwendung der Bildschirm-/Code-Sperre
- Zeitnahe Verlustmeldung
- Sicherer Remote-Zugriff auf das Netz der Institution
- Sichere Nutzung von öffentlichen WLANs
- Sicherer Umgang mit mobilen Datenträgern
- Verschlüsselung tragbarer IT-Systeme und Datenträger
- Sicheres Vernichten von schutzbedürftigen Materialien und Dokumenten

essentiell

CON.7: Informationssicherheit auf Auslandsreisen (bund.de)

# Beispiel: Konzept für Auslandsdienstreisen nach BSI


- Einsatz von Diebstahl-Sicherungen
- Mitnahme notwendiger Daten und Datenträger
- Kryptografisch abgesicherte E-Mail-Kommunikation

Stand der Technik

- Abstrahlsicherheit tragbarer IT-Systeme
- Integritätsschutz durch Check-Summen oder digitale Signaturen
- Verwendung vorkonfigurierter Reise-Hardware
- Eingeschränkte Berechtigungen auf Auslandsreisen

Erhöhter Schutzbedarf

CON.7: Informationssicherheit auf Auslandsreisen (bund.de)

# Beispiel: Konzept für Auslandsdienstreisen nach BSI


Die „Initiative Wirtschaftsschutz“ gibt auf ihrer Website unter

Wirtschaftsschutz - Startseite

(https://www.wirtschaftsschutz.info)

weiterführende Informationen zur Sicherheit auf Geschäftsreisen.

# Wie machen es die OEMs?

**TISAX:** (Trusted Information Security Assessment Exchange)

Ein von der Automobilindustrie definierter Standard

Grundlage: ISO 27001

**Ziele:**

- Informationssicherheit, Datenschutz und Prototypenschutz für Unternehmen der Automobilbranche
- Austausch von Angaben über das Niveau der Informationssicherheit der Beteiligten.
- Anpassung der Informationssicherheit direkt auf die Automobilbranche

**Also:**

Das geforderte Niveau der Informationssicherheit soll

- prüfbar
- dokumentierbar
- nachweisbar

sein.

# Wie machen es die OEMs?

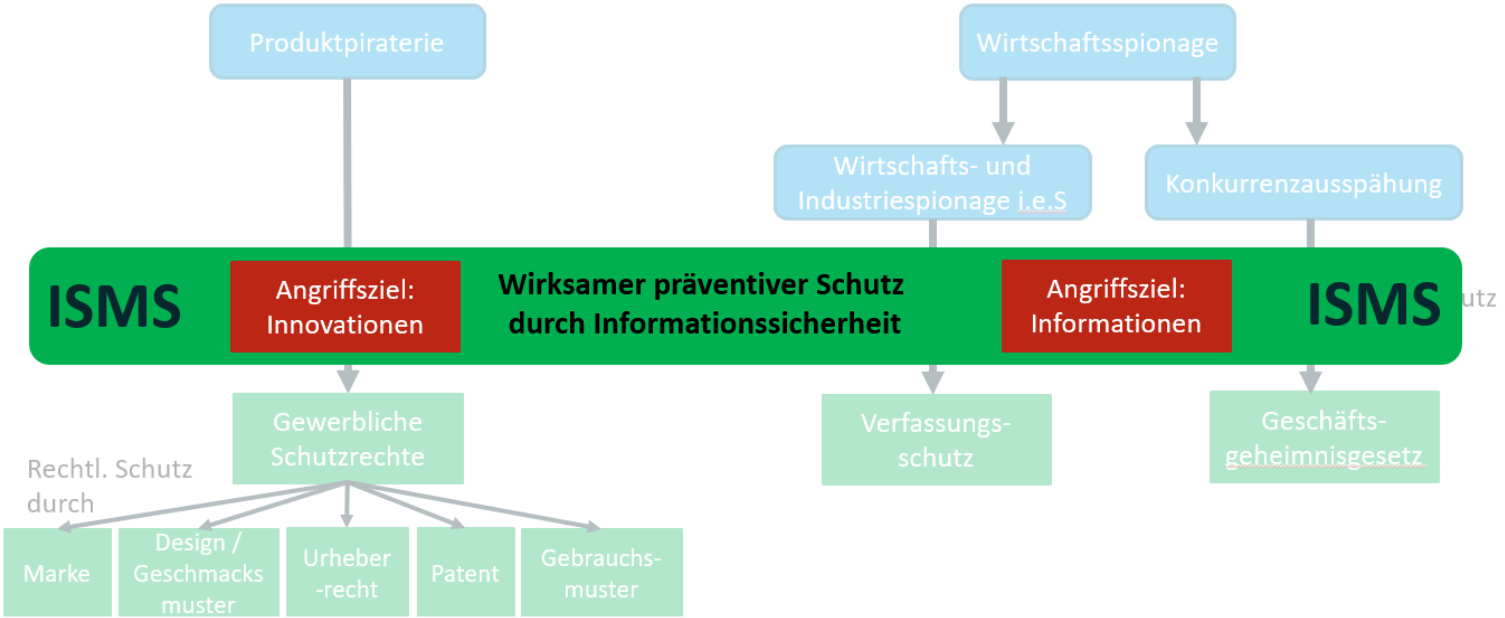
## TISAX: Zusammenhang zwischen Prüfziel und Assessment-LevelX

| Nr | Prüfziel | Abkürzung | AL |
|---|---|---|---|
| 1 | Informationen mit hohem Schutzbedarf | Info high | AL 2 |
| 2 | Informationen mit sehr hohem Schutzbedarf | Info very high | AL 3 |
| 3 | Datenschutz gemäß Art. 28 DSGVO (Auftragsverarbeiter) | Data | Al 2 |
| 4 | Datenschutz gemäß Art. 28 DSGVO (Auftragsverarbeiter) bei besonderen Kategorien personenbezogener Daten | Special data | AL 3 |
| 5 | Schutz von Prototypen-Bauteilen und –Komponenten | Proto parts | AL 3 |
| 6 | Schutz von Prototypenfahrzeugen | Proto vehicles | AL 3 |
| 7 | Umgang mit Erprobungsfahrten | Test vehicles | AL 3 |
| 8 | Schutz von Prototypen während Veranstaltungen und Film- und Fotoshootings | Event + shootings | AL 3 |

# Agenda

1. Einführung in das Thema
2. Auswirkungen der Produktpiraterie auf die Unternehmen
3. Schutz vor Produktpiraterie
4. Wirtschaftsspionage / Ransomware
5. Informationsklassifizierung und weitere Schutzmaßnahmen
6. Fazit

# Fazit


Produktpiraterie
Wirtschaftsspionage
Wirtschafts- und Industriespionage i.e.S
Konkurrenzausspähung
ISMS
Angriffsziel: Innovationen
Wirksamer präventiver Schutz durch Informationssicherheit
Angriffsziel: Informationen
ISMS
Gewerbliche Schutzrechte
Verfassungs-schutz
Geschäfts-geheimnisgesetz
Rechtl. Schutz durch
Marke
Design / Geschmacks muster
Urheber -recht
Patent
Gebrauchs-muster