PEak News@BDO

Watch out, Private Equity: That´s how they hack you!

April 2023

Ein (allzu oft realer) Cybercrime Thriller

von Franziska Hain

Disclaimer: Die Handlung und alle handelnden Personen sind frei erfunden. Jegliche Ähnlichkeit mit lebenden Personen oder realen Unternehmen wären rein zufällig.

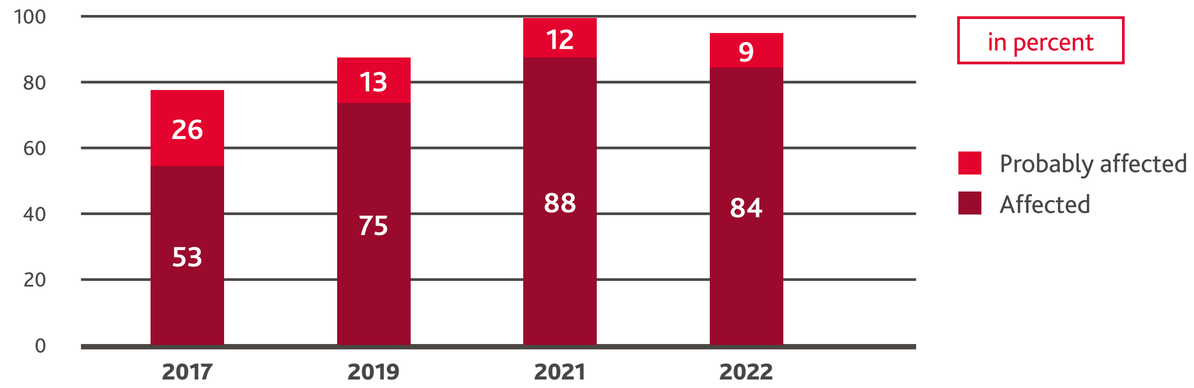
My day is off to a great start with a new message: „Hey Dude, I need your help. It's about that German competitor of ours, Schumpeter´s Creative Destruction AG (SCD) – one of The Next Unicorn Private Equity (TNU PE)´s portfolio companies. It seems they have just successfully launched an absolute breakthrough product innovation in consumer robotics. If this is true, our market cap will melt down like Fukushima. Disastrous for the value of my shares in Zombie Inc., and we´re so close to the merger right now. Is there anything you can do?“

My heart leaps. Immediately my brain starts rattling. And slowly but surely, I draw my plans against them.

I say „surely“ as more than 90% of German companies are wide open to top hackers like me:

German economy affected by attacks across the board

Has your company been affected by theft, industrial espionage or sabotage within the last 12 months? (2017 and 2019: within the last two years)



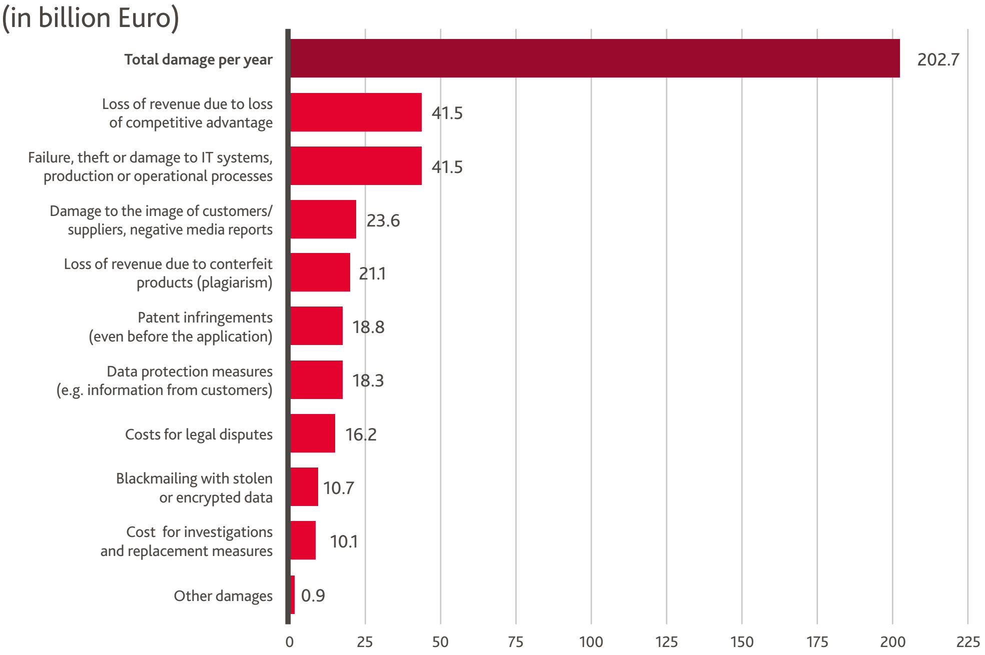
Bitkom Study: 9 out of 10 companies in Germany are victims of data theft, espionage or sabotage.
Source: Bitkom

First, I need to gain more information on SCD and TNU Private Equity using search engines for the web and the darknet. I can easily access the darknet in a stealth operation via the **Tor browser**. It protects me from being discovered or identified. I need to know, for example, who the Head of R&D at SCD is, and usually, I will be able to find that information on social media. I also need to find out how to attack SCD/TNU. So, I´ll do some research on the servers, websites and locations they use. And I´ll use **shodan.io** to hunt down any IoT devices they have that are accessible through the web. Once I have gained an overview, I´ll consider the most promising path of attack. Since we are aiming to access the R&D documents of their new product, a dual track target strategy would seem the best way forward: SCD´s Head of R&D first, and then the relevant investment director at TNU PE.

First of all, I´ll send a perfidious **phishing email** to the Head of R&D. Best practice in my business. 95% of all successful cyberattacks are based on human failure, which is mainly triggered by spear phishing. There is a wealth of examples in the darknet showing what phishing emails should look like to maximize the probability of success. I´ll pick the most suitable one for my target and adapt it to make it as personalized as possible, utilizing potential weaknesses such as curiosity, fear or greed. The more personal, the more credible, and, thus, the higher the probability that the person in question will get caught out. That takes time. Information on social media is particularly helpful here. Surely not the reason, why they put it there, I think grinning to myself. They would´nt be that naive if they were aware of the damage caused by attacks in Germany by members of my profession:

Damage from cybercrime in Germany in 2022

(in billion Euro)



Source: Statista 2023

Hopefully, I can get him to enter his login details on my website. I´ll design a perfect copy of SCD´s site to cover the fake. If he enters his credentials here, he´ll be trapped and I can use them later to log in myself.

After he has fallen for my trick, I´ll need to see whether I can gain access to one of the servers. This should work, if they use outdated software with known vulnerabilities. There are many so-called **exploits** on the internet that I can utilize and adapt. That´s a no-brainer, as exploits are delivered with appropriate descriptions. I only need to adjust the IP address to target the right server. If their configurations are completely amateurish, I will even be able to gain access without an exploit. Happens more often than one might think. IT departments are generally under-staffed and budgets too low.

As soon as I have access to the server, I need to penetrate deeper into the internal network. Drawing on my experience I will gradually expand my rights via further attacks. The easiest way is, if I manage to log on to a Windows computer as a normal user. I´ll try to gain administrator rights on this computer via the usual suspects: Vulnerabilities - and trust me, there are almost always some to be found. As an administrator, I will then have critical mass to hijack the entire network. Quantum leaps can be catalyzed by the **Metasploit** tool which contains many pre-programmed attack vectors. With the ultimate objective now firmly in view, i.e. to log in with the stolen credentials, I will finally gain access to the files, emails, etc. of the Head of R&D. Even better, I might obtain the highest possible level of authorization. Then, the internal network will belong to me and I can access virtually everything.

Of course, I will also install **hidden malware** that allows me to come back later, even if the login details have been changed or vulnerabilities have been fixed. Who knows what useful information will come up later? Not to mention the fact that I will install the whole thing in a way that is as well buried as possible, so that no one will notice.

Even if none of that should work, I´ll tackle a multitude of employees with a **multi-channel-phishing** attack containing some pretty awesome ransomware links. The goal here will be to block core R&D results of the new product development and to blackmail SCD. Nice IRR on my $1,900 annual darknet investment in **Ransomware-as-a-service**! And great that it includes major measures to ensure that users remain undetected. Who´s worried about law enforcement? The general risk of being caught is extremely low. Very useful!

> Only the dumb 5% of cyber criminals ever get caught. Exposing themselves with expensive sports cars and stuff. How stupid. Couldn´t happen to me.
>
> With a diabolic grin on my face, I quickly reply: „Sure, piece of cake. You know my conditions – you can count on me!“ As if he had desperately been waiting for an answer, he immediately confirms the mandate: „Great, go for it! Right away! Thanks!“

Fünf Tage nach dem erfolgreichen Angriff:

„Dies ist das erste deutsche Fernsehen mit der Tagesschau.

Heute wurde das US-amerikanische Unternehmen Zombie Inc. für den Rekordwert von 26 Milliarden US-Dollar übernommen. Grund für die hohe Bewertung ist der jüngste Durchbruch in der Entwicklung eines innovativen Produkts im Bereich sogenannter Consumer Robotics. Laut Expertenmeinungen wird dieser Durchbruch unseren Alltag nachhaltig verändern. Der Kurs des deutschen Wettbewerbers SCD AG fiel heute nach Veröffentlichung der Übernahme auf ein Allzeittief…“

Autorin:

Franziska Hain
Geschäftsführerin BDO Cyber Security GmbH
franziska.hain@bdosecurity.de

BDO Cyber Security Services für Private Equity

- Zentrale Cyber Security Schutzleistungspakete für GPs/PE-Portfolien
- Schutzschirm-Outsourcing auf BDO Cyber Security Managed Services
- Minimierung des multiplen Angriffsrisikos auf Werte von GPs/ Portfolio-Unternehmen
- Betrieb von BDO Cyber Security Operations Center (SOC)

Strategic Risk Management

- Strategische Beratung
- Cyber Versicherungen
- Business Model Risk Assessment
- Cyber Risk Assessments

Security Operations Center

- SOC as a Service
- Incident Response
- Digitale Forensik
- Threat Hunting & Intelligence

Management-Systeme

- Informationssicherheitsmanagement
- Business Continuity Management
- Datenschutzmanagement
- Branchenspezifische Standards
- Auditierung und Zertifizierung

Identity Governance

- Identity & Access Management
- Privileged Account Management
- Customer Identity and Access Management

Security Architecture & Design

- Enterprise Security Architecture
- Development, Security and Operations
- Secure Development Lifecycle
- Operational Technology Security

Cyber Incident Response & IT-Forensics

- Notfall-Support (24/7)
- Rettungsmaßnahmen
- Schadenermittlung (IT-Infrastruktur)
- Rechtsberatung und Krisenkommunikation

Offensive Security Services

- Vulnerability Assessments
- Penetration Testing
- Simulated Social Engineering
- Open Source Threat Intelligence
- Schulungen, Phishing-Simulationen

Data Protection / Privacy

- GDPR / EU-DSGVO
- Data Privacy Officer
- Privacy by Design / Default
- Data Classification

BDO AG Wirtschaftsprüfungsgesellschaft
Fuhlentwiete 12
20355 Hamburg
www.bdo.de

Ihre Private Equity-Ansprechpartner:

Dr. Michael Brauer
Tel.: +49 211 1371-186
michael.brauer@bdo.de

Dr. Jan Faßhauer
Tel.: +49 69 95941-463
jan.fasshauer@bdo.de

Dietmar Flügel
Tel.: +49 211 1371-162
dietmar.fluegel@bdo.de

Michael Maxeiner
Tel.: +49 211 1371-185
michael.maxeiner@bdo.de

Thorsten Schumacher
BDO Legal
Rechtsanwaltsgesellschaft mbH
Tel.: +49 211 1371-323
thorsten.schumacher@bdolegal.de

Die Informationen in dieser Publikation haben wir mit der gebotenen Sorgfalt zusammengestellt. Sie sind allerdings allgemeiner Natur und können im Laufe der Zeit naturgemäß ihre Aktualität verlieren. Demgemäß ersetzen die Informationen in unseren Publikationen keine individuelle fachliche Beratung unter Berücksichtigung der konkreten Umstände des Einzelfalls. BDO übernimmt demgemäß auch keine Verantwortung für Entscheidungen, die auf Basis der Informationen in unseren Publikationen getroffen werden, für die Aktualität der Informationen im Zeitpunkt der Kenntnisnahme oder für Fehler und/oder Auslassungen.

BDO AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft deutschen Rechts, ist Mitglied von BDO International Limited, einer britischen Gesellschaft mit beschränkter Nachschusspflicht, und gehört zum internationalen BDO Netzwerk voneinander unabhängiger Mitgliedsfirmen.
BDO ist der Markenname für das BDO Netzwerk und für jede der BDO Mitgliedsfirmen.

BDO Legal Rechtsanwaltsgesellschaft mbH, eine Gesellschaft mit beschränkter Haftung, ist rechtlich selbständiger Kooperationspartner der BDO AG Wirtschaftsprüfungsgesellschaft.
BDO AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft deutschen Rechts, ist Mitglied von BDO International Limited, einer britischen Gesellschaft mitbeschränkter Nachschusspflicht, und gehört zum internationalen BDO Netzwerk voneinander unabhängiger Mitgliedsfirmen.
BDO ist der Markenname für das BDO Netzwerk und für jede der BDO Mitgliedsfirmen.

BDO Cyber Security GmbH, eine Gesellschaft mit beschränkter Haftung deutschen Rechts, ist eine rechtlich selbständige Konzerngesellschaft der BDO AG Wirtschaftsprüfungsgesellschaft. BDO AG Wirtschaftsprüfungsgesellschaft, eine Aktiengesellschaft deutschen Rechts, ist Mitglied von BDO International Limited, einer britischen Gesellschaft mit beschränkter Nachschusspflicht, und gehört zum internationalen BDO Netzwerk voneinander unabhängiger Mitgliedsfirmen.
BDO ist der Markenname für das BDO Netzwerk und für jede der BDO Mitgliedsfirmen.