

CYBER-BOOTCAMP AM 16. OKTOBER | 09:30 BIS 10:15 UHR

Cyber-Crime hautnah: Ein Blick ins Darknet und die Risiken für Unternehmen



NIKOLAUS STAPELS

Cyber-Security-Spezialist



DARKNET

Nikolaus Stapels

Schön, dass Ihr heute hier seid!

Nikolaus Stapels

Ich bin Nikolaus Stapels, Gründer der NSCT, Vertriebssoftware24 GmbH für Softwareentwicklung, SecuMetrix und der CyCo Cyber Competence Center GmbH für die Schadenbearbeitung von Cyberschäden in Deutschland.

Wir betreuen ca. 11.000 Unternehmen sowie 12.000 Haushalte im Bereich Cyber-Awareness.

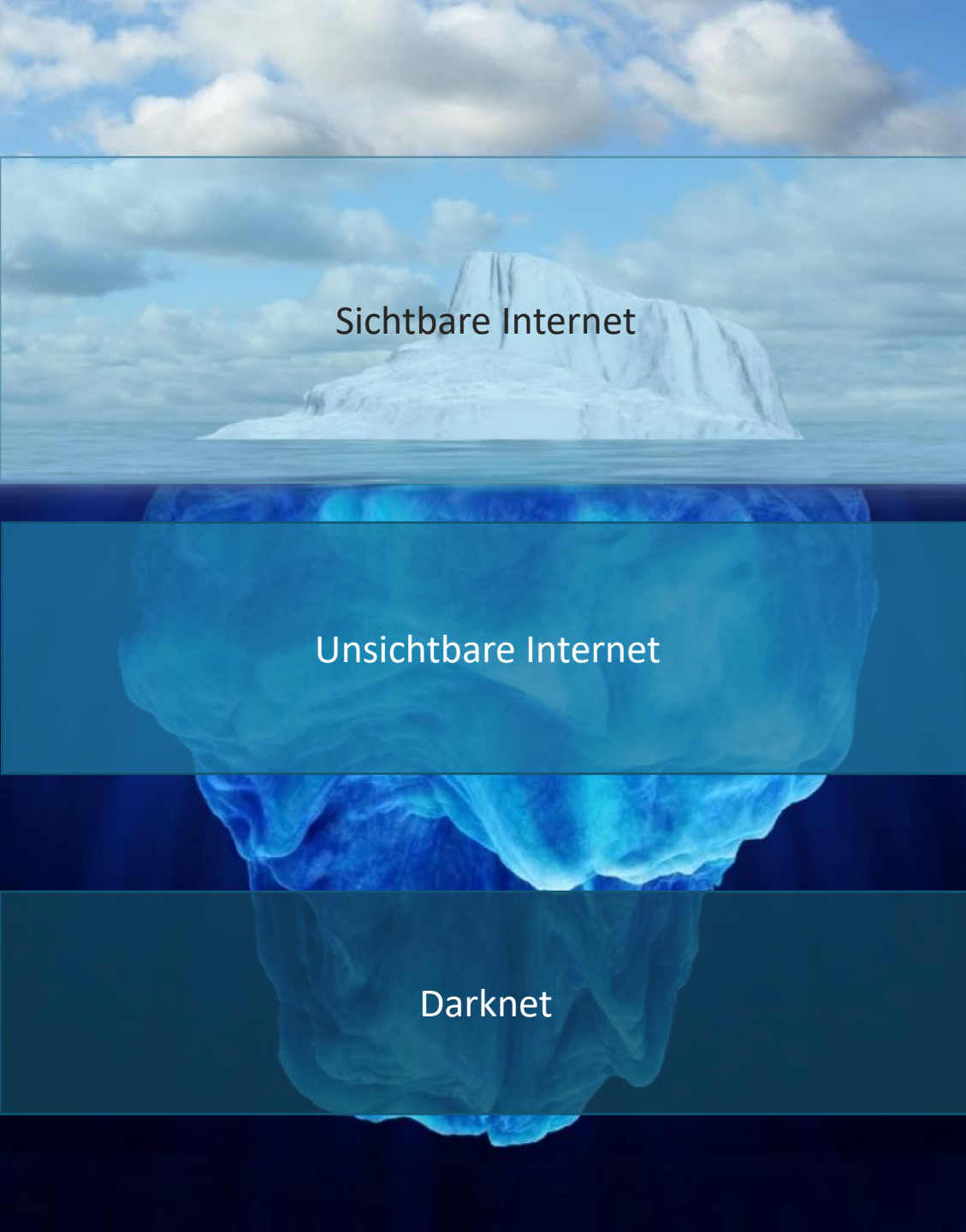
Des Weiteren unterstützen wir Unternehmen bei der Prävention mit Cyberscans, PenTesting und Notfallmanagement.



Eisbergmodell

Das Internet lässt sich gut anhand des **Eisbergmodells** erklären.

- Im oberen Bereich ist das „**sichtbare Internet**“, das macht 4% des gesamten Internets aus.
- Unter der Oberfläche befindet sich das „**unsichtbare Internet**“ auch „**Deep Web**“ genannt, dort gelangt der Nutzer nur hin, wenn er sich in einen internen Bereich einloggt, z.B. auf Ebay oder Amazon.
- Und unter dem Eisberg gibt es das s. g. „**Darknet**“, dort gelangt der Nutzer nur mit einer speziellen Software hin, dem „**TOR-Browser**“. Nutzer sind dort anonym unterwegs, was viele Kriminelle ausnutzen.



Wie funktioniert “Tor”

- Tor (The Onion Router) erlaubt es Nutzern, anonym zu surfen
- Es funktioniert dezentral mit Relaisstationen, anstatt eine direkte Verbindung aufzubauen
- Durch das Verbinden zu verschiedenen Servern wird die eigene IP-Adresse verborgen
- Freie Meinungsäußerung für Dissidenten und Journalisten

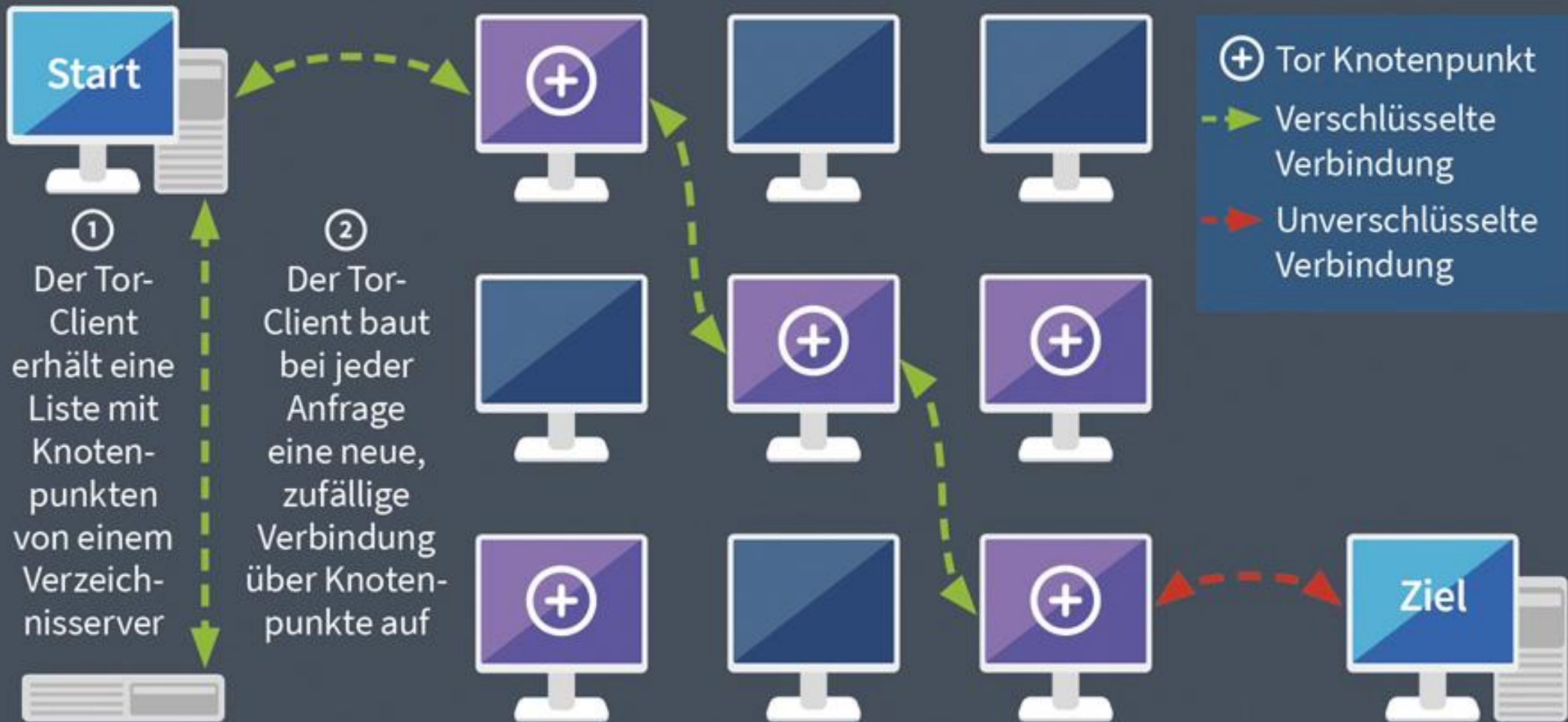
Nachteile

- Die Surfgeschwindigkeit wird verlangsamt
- Viele Regierungen sind skeptisch, was die Nutzung des Browsers angeht und überwachen gezielt die Onlineaktivitäten von den Nutzern
- Kriminelle können dort ihre Spuren verwischen





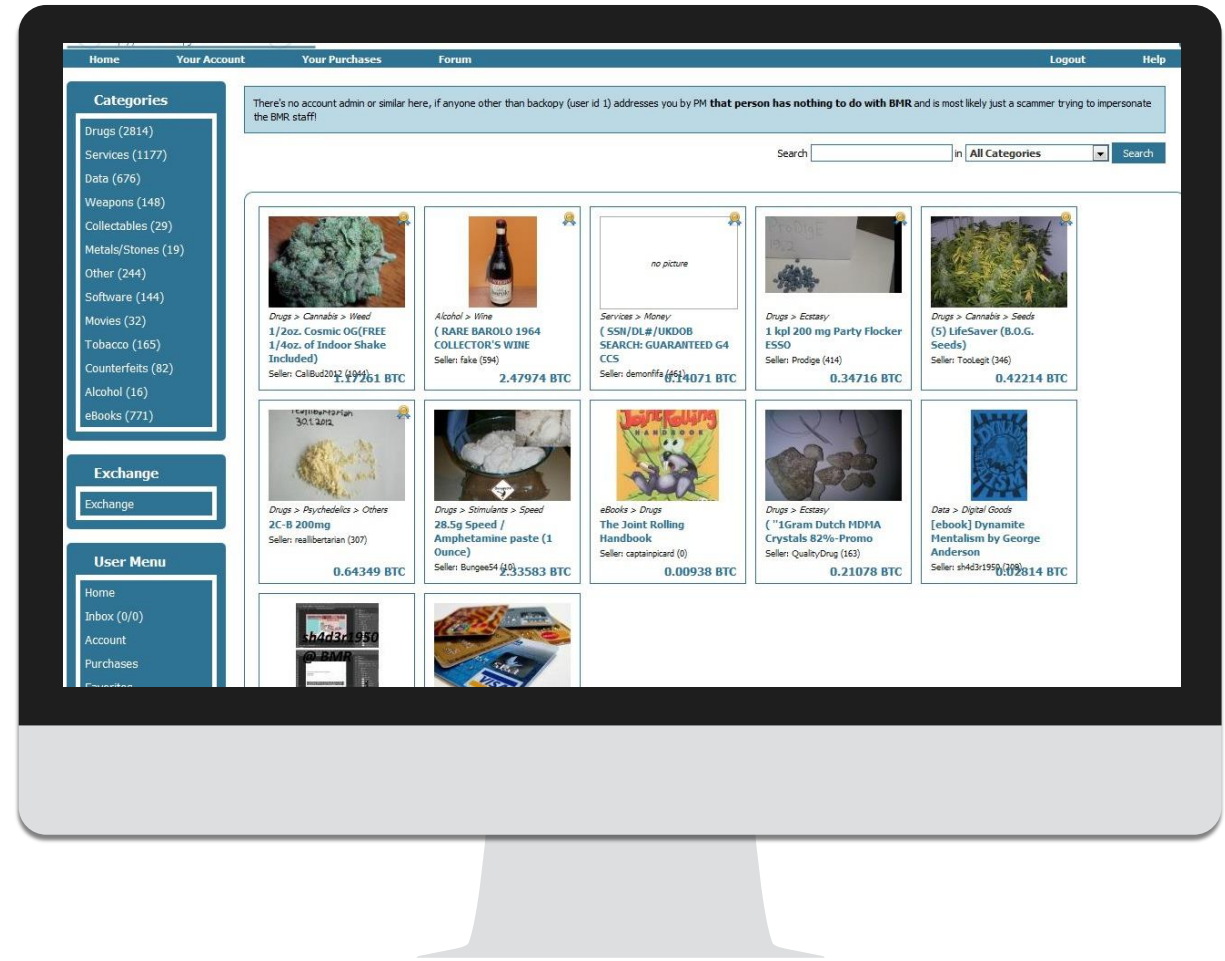
Wie funktioniert das **Tor**-Netzwerk?



Gefahren!

Beim Surfen auf illegalen Seiten muss jeder Nutzer Vorsicht walten lassen. Wer sich zum einen auf **verlockende (illegale) Angebote** einlässt, macht sich **strafbar** und riskiert Geld- sowie Haftstrafen.

Zum anderen kann der Besuch einer falschen Seite dazu führen, dass **Schadsoftware heimlich installiert** und der Rechner dadurch „verseucht“ wird.



Darknet - Schwarzmarkt

Die Märkte im Darknet spiegeln die **Entwicklung des freien Marktes** wider.

Die Märkte zeichnen sich durch **Innovationen** und **Wachstum** aus.

Es gibt **verschiedene Interessengruppen**, Industrien und Dienstleistungssektoren. Der Markt hat sich von einer Landschaft von einzelnen Hackern zu einer Spielwiese für **finanzgetriebene und gut organisierte Gruppen** entwickelt.

Ebenso wie im freien Markt gibt es viele qualifizierte und nicht qualifizierte Anbieter und Zwischenhändler für Dienstleistungen und Waren aller Art.

Zuverlässigkeit

Genau wie auf dem freien Markt sind die meisten Anbieter im Darknet, was die **Qualität und Art** des Produktes angeht, **ehrlich** - das mag komisch klingen, denen ist aber die Kundenzufriedenheit sehr wichtig.

Aber auch im Darknet gibt es **schwarze Schafe**, die locken Käufer mit falschen Angeboten und liefern keine Ware. Doch diese Anbieter verschwinden immer schneller, es scheint eine Art **Überwachung** stattzufinden.

Es ist ein starker personeller Zuwachs bei der Gruppe von **Cyberbanden** zu verzeichnen.



Struktur / Organigramm einer kleinen Hackergruppe





Dienstleistungs- sektor

Es werden im Darknet auch viele **Dienstleistungen** angeboten. In den letzten Jahren ist die Anzahl von Botnetzen gestiegen, dadurch können diese **DDoS-Attacken oder Spam-Kampagnen** als Service anbieten.

Bei vielen Angriffen wird die dafür notwendige Software nur „**gemietet**“, dadurch sparen die Kriminellen Geld, da sie die Software nicht selber entwickeln müssen.

So wie man jemanden beauftragt, seine Versicherungen zu prüfen, kann man im Darknet auf den Hacker-Schwarzmärkten für schmales Geld eine **Dienstleistung einkaufen**.



OZONE

Remote control program

Standard Package

Platinum Package

The most powerful Remote Control Program on the market
Demonstration [YouTube VIDEO](#)

Prices and Packages

We ❤️ our customers!



Right after purchase you
get a video tutorial!

Standard Package

1 month license

Live support
through chat & teamviewer

Free Updates

\$20

Platinum Package

Lifetime License

Live support
through chat & teamviewer

Bonus:

- MS Word .doc Exploit Builder
- Crypto Miner (multi engine, C++)

~~\$100~~

\$50

SALE!

Want to buy now? Click the thread to purchase.



Beispiel

Ransomware as a Service – „Satan“

Ransomware

Wer bereit ist, einen **Pakt mit dem Teufel** einzugehen, kann sich im Darknet einen eigenen und personalisierten Verschlüsselungstrojaner zusammenstellen.

Die Software erlaubt es den Käufern, über eine Weboberfläche den Schadcode seinen **Bedürfnissen anzupassen**. So hat der Käufer die Möglichkeit, die Höhe des Lösegelds sowie die Botschaft anzupassen.

Die Erstellung der Software ist **kostenlos**, wenn aber ein Opfer zahlt, dann behält der Entwickler **30%** des eingenommenen Geldes ein - für seinen Service.

Dafür erhält der Käufer - neben dem Trojaner - auch **Word-Makros, Hilfe-Dateien** und einen umfassenden **Service**.

Das Einzige, worum der Käufer sich jetzt nur noch kümmern muss, ist die Verteilung des Trojaners.





Version 2.1 Beta

[+] Tool Created by htr-tech (tahmid.rayat)

[::] Select Any Attack for Your Victim [::]

[01] Facebook	[11] Twitch	[21] DeviantArt
[02] Instagram	[12] Pinterest	[22] Badoo
[03] Google	[13] Snapchat	[23] Origin
[04] Microsoft	[14] LinkedIn	[24] CryptoCoin
[05] Netflix	[15] Ebay	[25] Yahoo
[06] Paypal	[16] Dropbox	[26] Wordpress
[07] Steam	[17] Protonmail	[27] Yandex
[08] Twitter	[18] Spotify	[28] StackoverFt
[09] Playstation	[19] Reddit	[29] Vk
[10] Github	[20] Adobe	[30] XBOX

[~] Select an option: 5 

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) SMS Spoofing Attack Vector
- 8) Wireless Access Point Attack V
- 9) QRCode Generator Attack Vector
- 10) Powershell Attack Vectors
- 11) Third Party Modules

- 99) Return back to the main menu.

set>



EagleSpy

Clients

Apk Bulder

Logs

Clear Logs

Block List

Apk Dropper

Clients Folder

Support



On



On



On

EagleSpy Ultimate version 3.0

Screen avatar

Flag Name

Country

And Phone

EagleSpy

Licence Panel

Mr-Exploit

Mr-Exploit

OK

LOGIN



Port :

Key :

Selected :

CPU : 0%



Live Screen

Live Camera

Calls

Keylogger

Reader

Notifications

Microphone

Messages

Files

Admin

Volume high

Location

Applications

Self Delete

Clipper

Volume 0

Lock

UnLock

Contacts

Accounts

Open url

Injection

Logger

Auth Steal

Toast

Start/Stop

Port

Status

KEY

Remove

PORT

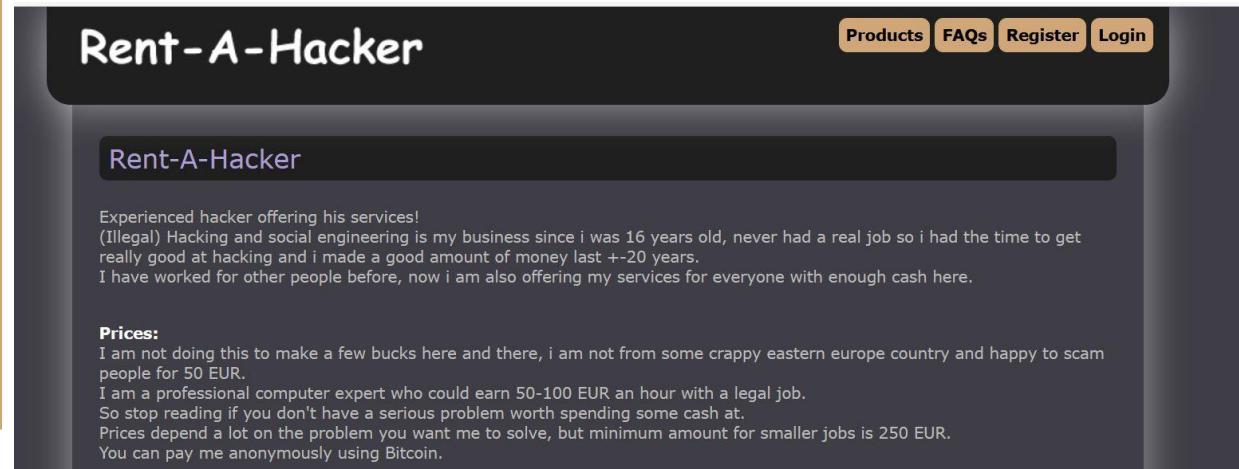
Add

EagleSpy

Rent A Hacker

Warum noch selber eine Unternehmen hacken?

Für bis zu 1.000 € bekomme ich die Experten, die ich brauche....



289 Milliarden Euro Schaden für die deutsche Wirtschaft

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2025)	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	73,3	54,5	35,0
Kosten für Rechtsstreitigkeiten	53,0	53,1	29,8
Kosten für Ermittlungen und Ersatzmaßnahmen	37,0	32,2	25,2
Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	30,6	39,2	15,3
Datenschutzrechtliche Maßnahmen, z.B. durch Behörden	23,8	27,2	12,4
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	23,1	11,2	21,5
Patentrechtsverletzungen, auch vor Anmeldung	16,0	14,8	10,4
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	15,9	20,2	35,3
Erpressung mit gestohlenen Daten	15,6	13,4	16,1
Geldabfluss durch Betrugsversuche	0,9	0,8	3,9
Sonstige Schäden	0	0	1,1
Gesamtschaden pro Jahr	289,2	266,6	205,9

4 Basis: Alle Unternehmen (n=1.002) | Mehrfachnennungen möglich | rundungsbedingt kann die Summe der Einzelschäden vom Gesamtschaden abweichen. | Quelle: Bitkom Research 2025

Gefahren der Digitalisierung

Buchungssystem

Online Buchungssystem (z.B.: Booking.com) oder eigene Webseite



Elektr. Schließsystem

Zugang zu Zimmer und anderen Räumen (z.B.: Heizraum,...)



Kundendaten

Persönliche Informationen und Daten der Gäste; Adressen, Kreditkarten, Geburtsdaten, ...



So schützen Sie Ihr Unternehmen besser

6 konkrete Maßnahmen für Unternehmer

1



MFA konsequent aktivieren

E-Mail, Banking, VPN und Admin-Zugänge zusätzlich absichern.

2



Backups testen

Offline oder unveränderbare Sicherungen vorhalten und die Wiederherstellung üben.

3



Mitarbeitende sensibilisieren

Phishing, CEO-Fraud und verdächtige Zahlungsaufforderungen regelmäßig trainieren.

4



Notfallplan festlegen

Klären: Wer entscheidet, wen rufen wir an und wie kommunizieren wir im Ernstfall?

5



Cyberanalyse durchführen

Cyberscan, Schwachstellenanalyse oder PenTest nutzen, um Risiken früh zu erkennen.

6



Cyberversicherung abschließen

Finanzielle Schäden abfedern und im Ernstfall schneller Spezialisten an Bord haben.



Ziel: Angriffe erschweren, Schäden begrenzen und schnell wieder arbeitsfähig sein.



Prävention und Hilfe im Schadenfall greifen ineinander.

FRÜH ERKENNEN. SCHNELL REAGIEREN. STARKER PARTNER. STABILISIEREN.



1 Präventiv

RISIKEN ERKENNEN UND REDUZIEREN



Analyse von außen

Bedrohungen erkennen,
Angriffsflächen aufdecken.



Analyse von innen

Schwachstellen identifizieren,
Sicherheitslage bewerten.



Mitarbeiterschulung

Bewusstsein stärken,
Risiken im Alltag reduzieren.

2

Im Schadenfall

SCHNELL. KOORDINIERT. MIT STARKEM PARTNER.



Notfallmanagement



schnell
reagieren



koordinieren



Betrieb
sichern



Cyberversicherung



Kosten übernehmen



24/7 Experten-Team



Forensik & Krisenhilfe



Wiederanlauf
unterstützen

3

Stabilisierung danach

ERHOLUNG UND ZUKUNFTSSICHERHEIT



Wiederaufbau beschleunigen

Systeme und Prozesse
rasch wiederherstellen.



Widerstandskraft stärken

Sicherheitsmaßnahmen
nachhaltig verbessern.



aus Vorfällen lernen

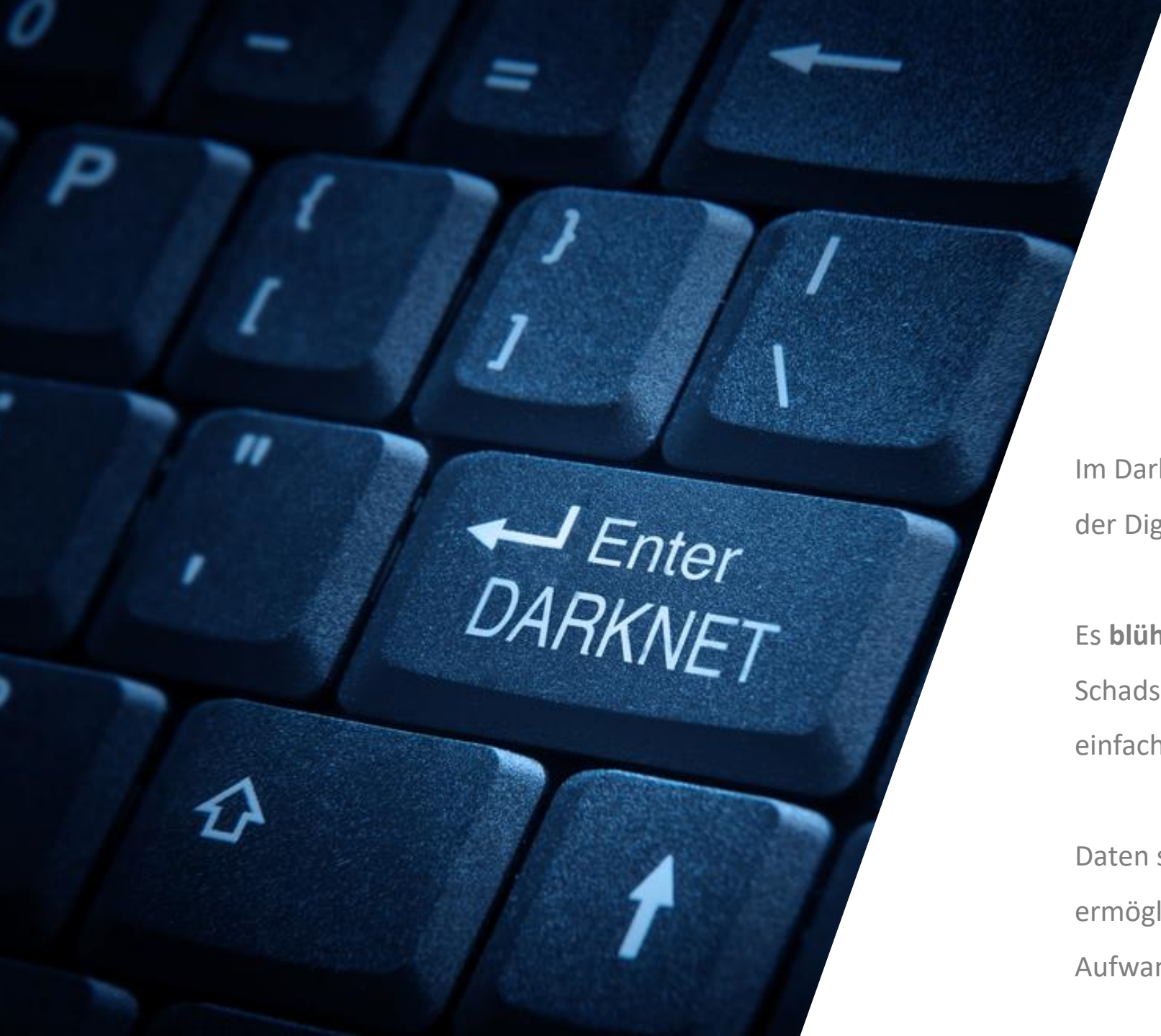
Erfahrungen nutzen
und dauerhaft besser aufstellen.



Gemeinsam prüfen,

welche Bausteine für Ihr Unternehmen sinnvoll sind.

Schreiben Sie uns:
info@secumetrix.de



Fazit?!?

Im Darknet sehen wir den technischen Fortschritt in der Digitalisierung von seiner **dunkelsten Seite**.

Es **blüht der Handel** mit hochsensiblen Daten und Schadsoftware; der Einstieg wird dabei immer einfacher.

Daten sind der Rohstoff des 21. Jahrhunderts und ermöglichen es Cyber Kriminellen, mit relativ wenig Aufwand viel Geld zu verdienen.

Fazit!?! ---

Cybercrime kann heutzutage jeder!

Wenn man von „Hackerangriffen“ und „Cybercrime“ hört, dann denken viele sofort an den typischen **Nerd**, der im Keller sitzt und das Tageslicht scheut.

Um als Täter aktiv mitmachen zu können, bedarf es weder tiefergehenden Wissens noch Programmierkenntnisse.

Jeder kann theoretisch innerhalb von **24 – 48 Stunden** eine kriminelle Laufbahn starten. Die nötigen Tools und Anleitungen finden sich schnell in Foren und auf Youtube.

JEDER Betrieb ist dadurch bedroht!

Nikolaus Stapels - info@stapels.consulting

