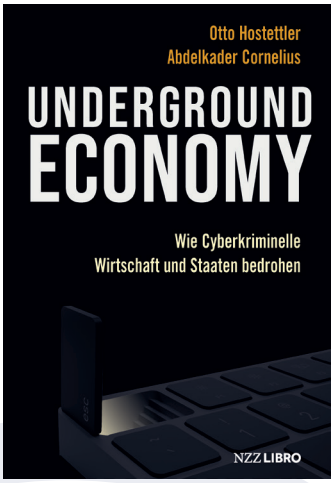
Einblicke in eine komplette Schattenwirtschaft – eine Buchrezension



Hostettler Otto, Cornelius Abdelkader, **Underground Economy. Wie Cyberkriminelle Wirtschaft und Staaten bedrohen**, 189 Seiten, Verlag NZZ Libro, Zürich 2022.

«With Love» steht auf der Website der Cybercrime-Gruppe «Vice Society». Dazu empfehlen sich ihre Mitglieder als «zuverlässige» Erpresser, die ihr Hacker-Hobby zum Beruf gemacht hätten und nach erfolgter Bezahlung die verschlüsselten Daten auch garantiert wieder «clean» freigeben würden. Diese angepriesenen Unternehmenswerte sind an Zynismus für den Lesenden von «Underground Economy» kaum zu überbieten, wobei diese Werte tunlichst zur Grundhaltung professionell agierender Cyberkrimineller gezählt sein wollen. Dank oftmals intrinsisch motivierter Triebfeder und in Kombination mit einem weit verzweigten, globalen, anonymen Netzwerk sind kriminell agierende Hacker – bis dato – den Cybercrime-Ermittlern meist einen Schritt voraus. Oder wie alt Bundesrätin Doris Leuthard im Vorwort des Buchs «Underground Economy» schreibt (S. 8): «Die immer grössere Zielscheibe von Organisationen im Netz wird begleitet von immer kompetenteren Angreifern. Denn die Cyberkriminellen haben, im Gegensatz zu manchen Firmen, in den letzten Jahren nicht geschlafen.»

Welche Entwicklungen von einer grossen Mehrheit verschlafen wurden und was nun getan werden kann beziehungsweise sollte, erklären die Autoren Otto Hostettler und Abdelkader Cornelius in ihrem Buch «Underground Economy. Wie Cyberkriminelle Wirtschaft und Staaten bedrohen» – eine Publikation, die brisanter nicht sein könnte, wird gegenwärtig und weltweit betrachtet doch inzwischen rund alle 11 Sekunden ein Unternehmen von Cyberkriminellen erpresst (zum Vergleich: 2015 soll dieser Wert noch bei 2 Minuten gelegen haben; vgl. S. 38).

Die «Underground Economy» erklärt

Für ihr Buch «Underground Economy» haben Hostettler und Cornelius mit Hackern, IT-Experten, Cybercrime-Spezialisten und Opfern von Cyber-Attacken gesprochen. Auf 170 Seiten geben sie Einblicke in die besorgniserregenden Entwicklungen der Hackerszene. In gut zugänglichem Reportage-Stil und mit eingestreuten, kurzen Fallbeschreibungen – beispielsweise von der ersten Schadsoftware «Brian» von 1986 bis hin zum perfiden Angriff auf das US-Unternehmen Colonial Pipeline im Frühling 2021 – erläutern die Autoren die Cybercrime-Entwicklung vom frühen, ausschliesslich experimentellen White-Hat-Hacking während den 1980er Jahren, auch Ethnical Hacking genannt, über Ransomware-Frühformen bis hin zu heutigen kriminellen Ausprägungen mit «Ransomware-as-a-Service»-Modellen. «Ransomware-Angebote gibt es inzwischen in verschiedensten Varianten, auf den einschlägigen Marktplätzen werden sie sogar mit Inseraten beworben. Denn: Die Konkurrenz funktioniert auch unter Erpressern», schreiben die Autoren (S. 86). Damit können Erpressergruppen, welche die Schadsoftware nicht selber programmieren wollen, bestehende (und bewährte) Malware als Paket mieten und allenfalls nach eigenem Bedarf weiterentwickeln (und erneut in erweiterter Form «zum Mieten» auf dem Markt anbieten). Die Autoren weiter: «Ein Testmonat gibt es für 120 Dollar, ein Sechs-Monate-Abo für 490 Dollar, und eine Jahresnutzung

Böhni Communications GmbH | Birkenstrasse 14 | CH-6003 Luzern
+41 79 725 72 61 | info@boehnicommunications.ch | www.boehnicommunications.ch

kostet 1900 Dollar. Das Paket umfasst alle verschiedenen Features, die nötig sind, um die Software auf dem Netzwerk der Firma zu platzieren, die Daten zu verschlüsseln, mit dem Unternehmen in Kontakt zu treten und die Daten schliesslich wieder zu entschlüsseln. Dazu selbstverständlich tadellosen Support. Der Return on Investment ist riesig.» (S. 86) Wobei Experten von einem ROI von mindestens 60‘000 Dollar monatlich ausgehen. Gewisse Erpresserbanden wollen ihre angewendete Ransomware gar aktiv optimieren, indem sie Belohnungen bezahlen, wenn andere Nutzer ihrer Software ihnen ausgemachte Schwachstellen oder Bugs (Fehler) melden – «Make Ransomware Great Again» dank Bug-Bounty-Programmen.[1]

Im Buch werden zwiespältige Berührungspunkte der «Underground Economy» mit weltweit operierenden Geheimdiensten angesprochen, der Einsatz von Cybercrime in Diktaturen beleuchtet, die Rolle von Kryptowährungen wie Bitcoin und Monero in diesem Kontext angeschaut und jüngste Entwicklungen wie die Corona-Pandemie als Digitalisierungs- und damit einhergehend auch als Cybercrime-Beschleuniger beschrieben – Stichwort Homeoffice als Einfallstor in Firmennetzwerke. All diese Brennpunkte können auf 170 Seiten natürlich nicht im Detail abgehandelt werden, aber als beeindruckende beziehungsweise beunruhigende Rundschau auf diesem Themengebiet muss die Lektüre von «Underground Economy» insbesondere den Themenneulingen nahegelegt werden. Denn nach der Lektüre ist klar, dass die Zeiten von Phreaking, Skript Kiddies und Crackern vorbei ist – Cybercrime ist eine hochprofessionelle Exploit-Industrie, vor der sich jede und jeder mit vorsorglichen, systematisch und konsequent umgesetzten Massnahmen früher, statt später zu schützen beginnen muss. Was ist zu tun?

Nach der Lektüre

Das letzte Kapitel von «Underground Economy» widmet sich der Frage, was man als Privatperson und als Unternehmen hinsichtlich der Internetnutzung vorsorglich tun kann, um sich vor Cyberattacken zu schützen. Themenaffinen Leserinnen und Lesern werden sich hier kaum neue Punkte eröffnen, zumal die meisten hiervon auch anderweitig in der medialen Berichterstattung immer wieder zu lesen sind. Doch steht und fällt das Präventionsanliegen dieses Buchs mit der Beherzigung dieser Tipps, wobei auch der Rezensent seine Hausaufgaben diesbezüglich nach dem Lesen von «Underground Economy» endlich hat anpacken müssen – namentlich ein erfolgter Wechsel des verwendeten Internet-Browsers sowie ein systematischer Einsatz von 32-stelligen, starken Passwörtern und eines Passwortmanagers (Firefox Lockwise mit Haupt- bzw. Master-Passwort ist eine Möglichkeit). Weitere Tipps wie regelmässige Backups auf externen Datenträgern, aktivierte Firewall, professioneller Virenschutz, regelmässige Durchführung der System-Updates und Awareness im Umgang mit Phishing- und Spam-Mails befolgt der Rezensent seit geraumer Zeit. Diese präventiven Massnahmen sind kein Sicherheitsgarant vor Cyberattacken – aber man kann es Angreifern deutlich und damit entscheidend schwerer machen.

Die Lektüre von «Underground Economy» – zumal gut zugänglich und von effizienter Textlänge – kann nur empfohlen werden. Den Autoren Otto Hostettler und Abdelkader Cornelius gelingt es, engagiert aber ohne einer Paniktonalität zu verfallen, die Lesenden wachzurütteln und ihnen kon-

Böhni Communications GmbH | Birkenstrasse 14 | CH-6003 Luzern
+41 79 725 72 61 | info@boehnicommunications.ch | www.boehnicommunications.ch

krete, im (Geschäfts-) Alltag mit überschaubarem Aufwand umsetzbare Massnahmenempfehlungen mit auf den Weg zu geben. Your move.

Luzern, 7. Juli 2022 / bb

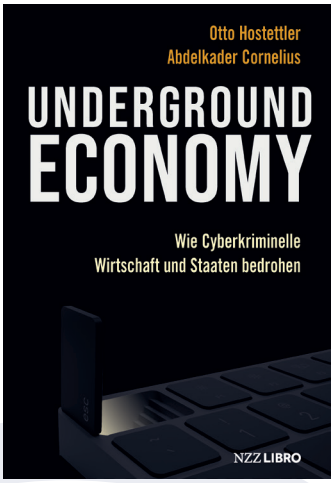
[1] Quelle: Dirk Knop, Lockbit-Ransomware-Gruppe stellt sich professioneller auf, online unter: https://www.heise.de/news/Lockbit-3-0-Professionalisierung-der-Ransomware-Szene-7155742.html (Stand: 7. Juli 2022).

Zum Autor der Rezension

Im Sommer 2018 gründete Basil Böhni (*1985) die Böhni Communications GmbH. Er studierte im Hauptfach Publizistik an der philosophischen Fakultät der Universität Zürich. Auf seinem bisherigen Berufsweg durfte sich Basil Böhni für verschiedene Arbeitgeber in den Bereichen interne Kommunikation, Öffentlichkeitsarbeit, Digital Marketing, Kultur, Event Management und Journalismus engagieren.

Böhni Communications GmbH | Birkenstrasse 14 | CH-6003 Luzern
+41 79 725 72 61 | info@boehnicommunications.ch | www.boehnicommunications.ch

Insights into an extensive underground economy – a book review



Hostettler Otto, Cornelius Abdelkader, **Underground Economy. Wie Cyberkriminelle Wirtschaft und Staaten bedrohen**, 189 pages, Verlag NZZ Libro, Zurich 2022.

„With Love“ is written on the website of the cybercrime group „Vice Society“. Its members recommend themselves as „reliable“ blackmailers who have turned their hobby of hacking into a profession and who, after payment, are guaranteed to release the encrypted data „clean“ again. These advertised corporate values are hard to beat in terms of cynicism for the reader of „Underground Economy“, although these values should preferably be counted as part of the basic attitude of professionally acting cyber criminals. Thanks to an often intrinsically motivated driving force and in combination with a widely ramified, global, anonymous network, criminally active hackers are – to date – usually one step ahead of cybercrime investigators. Or as former Federal Councillor Doris Leuthard writes in the foreword of the book „Underground Economy“ (p. 8): „The ever-increasing targeting of organisations on the net is accompanied by ever more competent attackers. Because the cybercriminals, unlike some companies, have not been asleep in recent years.“

The authors Otto Hostettler and Abdelkader Cornelius explain in their book „Underground Economy. How Cybercriminals Threaten the Economy and States“ what was missed so far in terms of prevention – a publication that could not be more relevant, given that currently and globally, a company is blackmailed by cybercriminals every 11 seconds (for comparison: in 2015, this figure was said to be 2 minutes; see p. 38).

The underground economy explained

FFor their book „Underground Economy“, Hostettler and Cornelius spoke with hackers, IT experts, cybercrime specialists and victims of cyberattacks. On more than 170 pages, they provide insights into the worrying developments in the criminal hacker scene. In an accessible reportage style and with interspersed short case descriptions – for example, from the first malware „Brian“ in 1986 to the perfidious attack on the US company Colonial Pipeline in the spring of 2021 – the authors explain the cybercrime development from the early, exclusively experimental white-hat hacking during the 1980s, also called ethnic hacking, to ransomware early forms to today‘s criminal manifestations with „ransomware-as-a-service“ models. „Ransomware offers now exist in a wide variety of forms, and they are even advertised on the relevant marketplaces. Because: competition also works among extortionists,“ the authors write (p. 86). This means that extortion groups that do not want to program the malware themselves can rent existing (and proven) malware as a package and, if necessary, develop it further according to their own needs (and offer it again on the market in an expanded form „for rent“). The authors continue: „A trial month is available for 120 dollars, a six-month subscription for 490 dollars, and a year‘s use costs 1900 dollars. The package includes all the various features needed to place the software on the company‘s network, encrypt the data, contact the company, and finally decrypt the data again. Plus, of course, impeccable support. The return on investment is huge.“ (p. 86) Whereby experts assume an ROI of at least 60,000 dollars per month.

Böhni Communications GmbH | Birkenstrasse 14 | CH-6003 Luzern
+41 79 725 72 61 | info@boehnicommunications.ch | www.boehnicommunications.ch

Some extortion gangs even want to actively optimize the ransomware they use by paying rewards when other users of their software report discovered vulnerabilities or bugs – „Make Ransomware Great Again“ thanks to bug bounty programs.[1]

The book addresses ambivalent touch points between the underground economy and globally operating intelligence services, highlights the use of cybercrime in dictatorships, looks at the role of cryptocurrencies such as Bitcoin and Monero in this context and describes recent developments such as the Corona pandemic as a digitalisation accelerator and thus also as a cybercrime accelerator – keyword home office as a gateway into company networks. Of course, it is not possible to cover all these hotspots in detail on 170 pages but the read of „Underground Economy“ opens up an impressive and even disturbing overview of this topic, especially for those new to the subject. Because after reading it is clear that the times of phreaking, script kiddies and crackers are over – cybercrime became a highly professional exploit industry from which everyone must start protecting themselves with precautionary, systematically and consistently implemented measures sooner rather than later. What is to be done?

After reading

The last chapter of „Underground Economy“ is dedicated to the question of what one can do as a private person and as a company regarding internet use in order to protect oneself from cyberattacks. Readers with an affinity for the topic will hardly find any new points here, especially since most of these can also be read elsewhere in media reports. However, the prevention goal of this book stands and falls with the heeding of these tips, whereby the reviewer also finally had to do his homework in this regard after reading „Underground Economy“ – namely a change of the Internet browser used as well as a systematic use of 32-digit, strong passwords and a password manager (Firefox Lockwise with a main or master password is one possibility). Other tips such as regular backups on external data carriers, activated firewall, professional virus protection, regular system updates and awareness in dealing with phishing and spam mails have been followed by the reviewer for quite some time. These preventive measures are no guarantee of security against cyberattacks – but they can make things much more difficult for attackers.

Reading „Underground Economy“ – especially as it is easily accessible and of convenient text length – can only be recommended. The authors Otto Hostettler and Abdelkader Cornelius succeed in shaking up the readers with commitment but without falling into a panic mentality, and in giving them concrete recommendations for measures that can be implemented in everyday (business) life with manageable effort. Your move.

Lucerne, 7 July 2022 / bb

About the author of the review

Basil Boehni (*1985) founded Boehni Communications Ltd in the summer of 2018. He majored in journalism at the Faculty of Philosophy of the University of Zurich. In his career to date, Basil Boehni has had the pleasure of working for various employers in the fields of internal communications, public relations, digital marketing, culture, event management and journalism.

[1] Source: Dirk Knop, Lockbit-Ransomware-Gruppe stellt sich professioneller auf, online unter: https://www.heise.de/news/Lockbit-3-0-Professionalisierung-der-Ransomware-Szene-7155742.html (date: 7 July 2022).

Böhni Communications GmbH | Birkenstrasse 14 | CH-6003 Luzern
+41 79 725 72 61 | info@boehnicommunications.ch | www.boehnicommunications.ch