IW-Kurzbericht Nr. 15/2022

Wie der russische Cyberkrieg deutsche Unternehmen bedroht

Vera Demary, 25.02.2022

Der russische Angriff auf die Ukraine fand schon lange vor dem aktuellen Angriff auf dem Boden, dem Wasser und in der Luft im Netz statt: Der Konflikt ist auch ein Cyberkrieg mit umfassenden Cyberangriffen. Dies kann sich auch auf deutsche Unternehmen auswirken.

Im Allgemeinen verfolgen Hacker mit ihren Angriffen auf die Systeme und Geräte von Privatpersonen, Unternehmen oder auch Staaten oft Ziele wie die persönliche Bereicherung, etwa durch Erpressung mittels Ransomware oder die Manipulation oder den Abfluss von Daten. Darüber hinaus werden Cyberattacken auch eingesetzt, um politische, strategische und militärische Ziele zu verfolgen. Einen solchen Cyberkrieg – englisch Cyberwarfare – führt Russland schon seit langem gegen die Ukraine und setzt Cyberattacken auch während des aktuellen Einmarsches ein. Es ist wahrscheinlich, dass Kollateralschäden in anderen Ländern nicht ausbleiben und auch Deutschland und die hiesigen Unternehmen betroffen sein werden.

Krieg mit Cyberattacken

Die Maßnahmen des Cyberkriegs sind vielfältig. Sie reichen von gezielter Falschinformation in sozialen Netzwerken über Spionage in den Daten, Systemen und der Hardware des Gegners und seiner Verbündeten bis hin zu Cyberangriffen, die der Sabotage von deren Informations- und Kommunikationsinfrastruktur oder sogar der physischen Zerstörung von Industrieanlagen oder ähnlichem (CSIS, 2022).

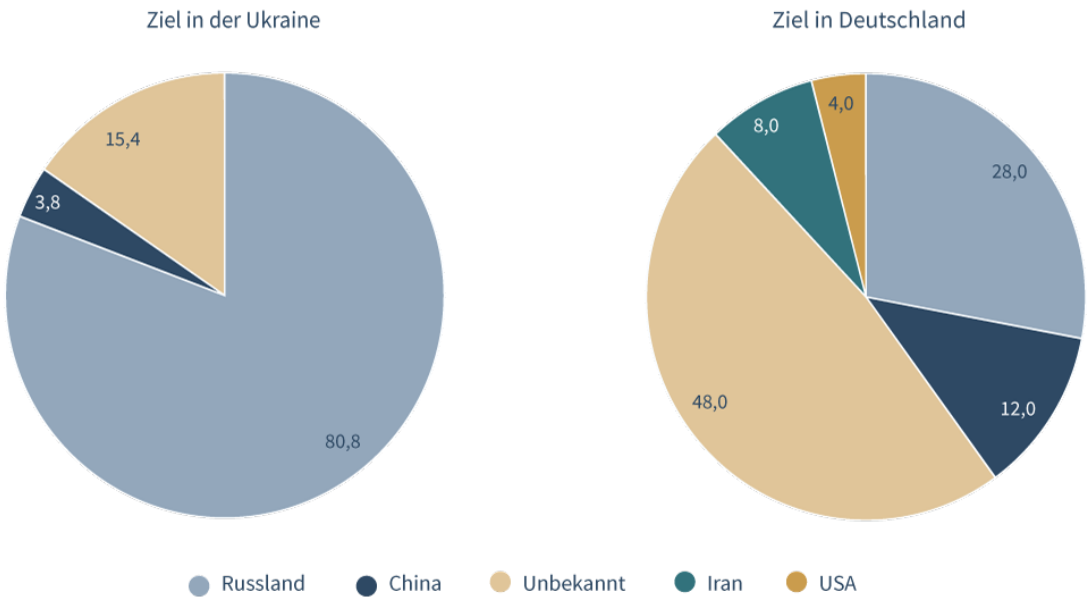
Ziele dieser Maßnahmen sind eine Schwächung des Gegners, die Demoralisierung der Bevölkerung und der ausländischen Öffentlichkeit und damit letztlich ein „Gewinn“ des Krieges und ein Erreichen politischer, strategischer oder militärischer Ziele. Dabei müssen die Angreifer selbst nicht unbedingt staatliche Akteure sein, sondern können auch von diesen geduldete, private Angreifer sein (CISA, o. J.).

Schon vor dem russischen Angriff auf die Ukraine ging der Großteil der auf ukrainische Regierungsbehörden, Verteidigungs- und High-Tech-Unternehmen verübten Cyberattacken auf das Konto russischer Akteure (Abbildung). Die Gesamtzahl der seit 2011 in der Datenbank des Center for Strategic and International Studies verzeichneten Cyber-Vorfälle in der Ukraine war ähnlich hoch wie der in Deutschland. Die Akteure unterschieden sich jedoch deutlich: Vier von fünf Cyberangriffen auf die Ukraine kamen aus Russland. In Deutschland konnte der Großteil der Angriffe keinem Staat zugeordnet werden. Russische Akteure machten 28 Prozent der Cyber-Vorfälle hierzulande aus.

Und auch während des laufenden Krieges sind ukrainische Behörden und Unternehmen immer wieder Ziel von Cyberangriffen: Die Websites von Banken und militärischen Organisationen wurden lahmgelegt. Eine Software, die systematisch Daten löscht, wurde auf hunderten Computern installiert (Tidy, 2022). Es kann davon ausgegangen werden, dass die Intensität dieser Attacken weiter zunehmen wird (Alazab, 2022).

Cyberattacken auf die Ukraine und auf Deutschland

Bedeutende Cyberangriffe auf Regierungsbehörden, Verteidigungs- und High-Tech-Unternehmen oder mit einem Schaden von mehr als einer Million Dollar, seit 2011, in Prozent der Angriffe



Stand: Januar 2022
Quelle: Eigene Berechnungen auf Basis von Center for Strategic and International Studies, 2022

Mögliche Auswirkungen auf Unternehmen in Deutschland

Der russische Cyberkrieg mit der Ukraine kann auch in andere Staaten ausstrahlen. Das Bundesamt für Sicherheit in der Informationstechnik BSI hat deutsche Unternehmen davor in dieser Woche gewarnt (Tagesschau.de, 2022). Die Gefahr besteht zum einen darin, dass Cyberangriffe auf die Ukraine sich nicht auf dortige Systeme, Hardware und Daten beschränken, sondern darüber hinaus auf verbundene Rechner in anderen Staaten verteilen. Die Schadsoftware „Petya/NotPetya“, die sich im Jahr 2017 über die Ukraine hinaus auch in den USA und Europa verbreitete, ist ein Beispiel für einen solchen Effekt (Alvarez de Souza et al., 2022). Zum anderen hat der russische Präsident Konsequenzen angedroht, wenn sich andere Staaten in den Krieg einmischen. Möglicherweise könnten demnach EU-Sanktionen gegen russische Unternehmen und Sektoren auch Cyberangriffe auf deutsche Unternehmen nach sich ziehen. Das Risiko dafür erscheint auch vor dem Hintergrund der BSI-Warnung erheblich.

Auch ohne diese zusätzliche Gefahr sind deutsche Unternehmen bereits jetzt oft das Ziel von Cyberangriffen. Im Jahr 2020 wurden für die deutsche Wirtschaft Schäden in Höhe von 223,5 Milliarden Euro durch den Diebstahl von Daten, Spionage und Sabotage geschätzt (Bitkom, 2021). Viele Cyberangriffe und auch die damit verbundenen Schäden in Unternehmen werden gar nicht erst gemeldet; es gibt also eine hohe Dunkelziffer. Die Auswirkungen solcher Vorfälle auf Unternehmen sind jedoch enorm: Zu den direkten Kosten für die Behebung des Schadens und den Verlust von Daten kommen indirekte Kosten beispielsweise für Umsatzausfälle oder Reputations- und Markenschäden (Engels, 2017, 12 ff.).

Das immense Schadensausmaß, das Cyberangriffe haben können, bestätigt auch eine Befragung des BSI: 26 Prozent der während der Pandemie von Cyberangriffen betroffenen Unternehmen gaben an, dass die Schäden sehr groß oder sogar existenzbedrohend waren (BSI, 2021, 17). Gleichzeitig strebten nur 16 Prozent eine Erhöhung ihres IT-Sicherheitsbudgets an (ebenda, 13). Dies ist angesichts der Gefährdungslage bedenklich. Um die Schäden im Falle eines Cyberangriffs gering zu halten, sind dringend resiliente IT-Sicherheitssysteme erforderlich – auch in Unternehmen, die nicht zu den kritischen Infrastrukturen gehören. Dafür sind Investitionen in smarte Sicherheitslösungen genauso erforderlich wie deren regelmäßige Überprüfung und Aktualisierung.

Literatur

Alazab, Mamoun, 2022, Russia is using an onslaught of cyber attacks to undermine Ukraine's defence capabilities, https://bit.ly/3ta47gD [25.2.2022]

Alvarez de Souza, Philipp / Holzki, Larissa / Karabasz, Ina, 2022, Hackerangriffe. Telekomchef Höttges warnt vor Cyberattacken in der Ukrainekrise: „Die Bedrohung ist da", https://bit.ly/3t4TnQB [25.2.2022]

Bitkom, 2021, Wirtschaftsschutz 2021, Berlin

BSI – Bundesamt für Sicherheit in der Informationstechnik, 2021, IT-Sicherheit im HOME-OFFICE, Bonn

CISA – Cybersecurity & Infrastructure Security Agency, o. J., Cyber Threat Source Descriptions, https://bit.ly/36GPJVx [25.2.2022]

CSIS – Center for Strategic and International Studies, 2022, Significant Cyber Incidents since 2006, Washington

Engels, Barbara, 2017, Wirtschaftliche Kosten der Cyberspionage für deutsche Unternehmen. Cybersicherheit als Grundvoraussetzung der digitalen Transformation, IW-Policy Paper, Nr. 6, Köln

Tagesschau.de, 2022, Ukraine-Krise. BSI warnt vor Cyberattacken, https://bit.ly/3t45H3G [25.2.2022]

Tidy, Joe, 2022, Ukraine crisis: 'Wiper' discovered in latest cyber-attacks, https://bbc.in/3pfrW5t [25.2.2022]