Börsen-Zeitung
Zeitung für die Finanzmärkte
Ausgabe 12 vom 20.01.2021, Seite 10

GASTBEITRAG

Cyberangriffe auf M&A: Risiken und Abwehr

Börsen-Zeitung, 20.1.2021
Cyberattacken auf Unternehmen sind weit verbreitet und ein lukratives Geschäft für die Angreifer. Im Schatten der aktuellen Cyber-Diskussion und weit unterschätzt von den Unternehmern sind Angriffe, die im Zuge von M&A stattfinden. In den vergangenen zwölf Monaten erlitten 96 % deutscher Unternehmen einen geschäftsschädigenden Cyberangriff. Das ergab eine Branchenstudie von Forrester Consulting, deren Ergebnisse im August 2020 vorgelegt wurden. Dieses Geschäft ist für die Angreifer höchst lukrativ – und mit relativ geringen Risiken behaftet, denn sie greifen geschützt aus dem Darknet an und lassen sich mit Kryptowährungen bezahlen. Mittlerweile hat sich eine ganze Cyberindustrie gebildet. Das „Marktvolumen", d. h. die Summe der Zahlungen durch Cyber-Erpressung, liegt weltweit bei 6 Mrd. Dollar.

Profis am Werk

Die „Gemeinschaften" sind hochprofessionell organisiert, etwa in Form von Franchising-Strukturen mit einem zentralen Treiber, der die Ziele auskundschaftet, also quasi Marktforschung, Kandidatenscreening, Priorisierung, Angriffe und Verfahren vorgibt. Dieser ist vernetzt mit externen „Methodikern", den eigentlichen Hackern, sofern er sie nicht schon an Bord hat: IT-Freaks, IT-Spezialisten und Hightech-Angreifer aus Spezialinstituten, die sich im Dunstkreis von Regierungen, Ministerien und Geheimdiensten befinden.

Angesichts hoher Verteidigungsmauern der Großkonzerne konzentrieren sich Cyber-Angreifer zunehmend auf die darunter liegende Schicht größerer mittelständischer Unternehmen. Hier sind die Hürden nicht ganz so hoch, die Aufmerksamkeit ist geringer. Der Aufwand für groß angelegte Einzelangriffe ist nämlich nicht unbeträchtlich. Deshalb sind die Angriffsziele im Sinne einer Aufwand-Risiko-Abwägung gut auszuwählen. Kleinere Mittelständler sind derzeit noch nicht das Ziel, denn sie verfügen nicht über die Geldmittel, die man erpressen kann und mit denen sich ein Angriff lohnt.

Obwohl die Aufmerksamkeit bei Konzernen und dem größeren Mittelstand auf die Beherrschung und Abwehr von Cyberangriffen durchaus gegeben ist, bleibt das Feld der Cybersicherheit vor, während und nach M&A-Transaktionen auf merkwürdige Weise weitgehend unbeachtet. Nur wenige Unternehmen haben dies auf ihrem Radar.

Angreifer haben M&A bereits als besonders günstige Gelegenheiten für Cyberattacken ausgemacht, insbesondere weil der Zeitdruck im Projekt, die Kommunikation, die Übergänge und Überführungen von unternehmerischen Aktivitäten viele Angriffsmöglichkeiten bieten – die sich bei genauerer Analyse von außen auch gut lokalisieren lassen.

Die spezifischen Schwächen und Risiken im Zuge von M&A sind hochprofessionellen Hackern meist schon grundlegend bekannt. Externe Profis durchleuchten die beteiligten Unternehmen im Vorfeld nach deren Sicherheitslücken. Leichtere Zutritte bieten die schwächeren Parteien in einem Deal. Ist hier erst einmal ein Zugang gelungen, kann der Angreifer abwarten, bis die IT-Systeme der Deal-Parteien zusammengeführt sind, und dann auch in das Netz des fusionierten Unternehmens eindringen, vielleicht sogar in die Architektur des besser geschützten Mutterkonzerns.

Angriffspunkte identifizieren

Sobald sich ein Deal ankündigt, lohnt es sich für Angreifer, sich mit dem Fall näher auseinanderzusetzen. Erste Signale liefert etwa ein Vorstand gegenüber der Presse zu seinen M&A-Absichten. Wenn ein Deal unter namentlicher Nennung des Kandidaten angekündigt wird, ist dies auch ein Startsignal für die genauere Planung von Attacken. Die Praxis zeigt, dass ein Ziel, das im Zuge von M&A angegriffen werden soll, systematisch durchleuchtet wird und dass professionelle Hacker zunächst strategische und operative Untersuchungen anstellen, bevor sie ihre teuren und fachlich herausfordernden Angriffe starten. Ihre Kernfragen sind, ob sich ein Angriff lohnen könnte, wie das Chancen-Risiko-Verhältnis liegt und wann sich der optimale Zeitpunkt für einen Angriff bietet. Das kann, wie Beispiele zeigen, auch Jahre nach der Übernahme sein.

Angesichts des massiven Anstiegs von Angriffen in Verbindung mit M&A sollten etwa Due Diligences auf Cyber-Themen ausgeweitet werden. Dazu gehören auch sogenannte Rapid Scans, die auf spezifische Schwachstellen ausgerichtet sein können. Diese dienen der Klärung des Sicherheitsprofils.

Derartige Untersuchungen sollten sich nicht nur auf externe Angreifer richten, sondern auch auf die Mitarbeiter. Gefährder sind Frustrierte, Verlierer und Gegner des Deals. Insbesondere die Phasen der Unsicherheit, Ängste vor Veränderungen und Furcht vor Jobverlust können bei M&A unerwartete Handlungen hervorbringen, auch Sabotage und Spionage von innen.

Nach dem Closing – wenn der Käufer erstmals vollen Zugang zu allen Ressourcen hat – sind weitere Prüfungen durchzuführen, nun durch direkten Zugriff im realen Objekt. Im Zuge eines Cyber-Risiko-Assessments können nun diejenigen Aktivitäten nachgeholt werden, die sich vor dem Closing rechtlich verbieten. So können sogenannte „White hat hatches" angeheuert werden, mit der Aufgabe, Netzwerke und Produkte zu „hacken" und „spots" zu entdecken, an denen Angreifer in das unternehmensinterne Netz eindringen können.

Sicherheit kostet Zeit

Zeitdruck und Hektik im M&A-Prozess generieren besondere Cyber-Risiken. Deshalb kann es nötig werden, die Geschwindigkeiten einzelner M&A-Prozesse temporär herabzufahren, eventuell sogar „Time-outs" zu vereinbaren, um Sicherheitslücken zu schließen. Das Ziel muss dabei sein, das Target auf ein höheres Sicherheitsniveau zu bringen.

Beobachtungen von Angriffen haben ergeben, dass professionelle Hacker systematisch Schwachpunkte beim (schwächeren) Target suchen, sich dort also einnisten. Sie schlagen erst dann los, wenn die Integration formell abgeschlossen ist. Dann hoffen sie, dass die IT-Systeme noch nicht harmonisiert sind und sie so durch die schwächeren Sicherungsfenster des bisherigen Targets in das neue integrierte Unternehmen eindringen können. Sie treffen dann die (bisher besser geschützte)

IT des wertvolleren und damit zahlungskräftigeren Übernehmers.

Zusammenfassend sollte sich ein Unternehmer, der sich auf einen M&A-Fall vorbereitet, einige Regeln zu Eigen machen:

- Bewusstsein schärfen: Cyber-Angreifer gehen systematisch vor. Sie kennen die spezifischen Cyber-Risiken bei M&A und nutzen diese systematisch aus.
- Spezifische Cyber Due Diligences mit Rapid Cyber Scans sollten zur Regel werden.
- Angesichts hoher potenzieller Vermögensschäden ist präventive Cyber-Abwehr bei M&A gut investiertes Geld.
- Im Vorfeld ist das spezifische Cyber-Risiko-Profil des jeweiligen M&A-Falles zu klären, denn jeder Fall birgt andere typische Gefahren.
- Halten Sie die IT-Verteidigungsmauern im gesamten M&A-Prozess hoch.
- Höchste Aufmerksamkeit ist angesagt, bei Erkennen erster Schäden schnell agieren: Bedrohte Abschnitte der internen Netze vom Internet trennen.
- Sicherheit im M&A-Projekt geht vor Geschwindigkeit: In besonderen Risikostadien lieber das M&A-Projekt unterbrechen oder Einzelprozesse aussetzen, als sich riskantem Zeitdruck auszusetzen.
- Wirtschaftlich besonders attraktiv sind Angriffe nach Abschluss des M&A-Projektes. Deshalb Aufmerksamkeit hochhalten!

Kai Lucks, Vorstandvorsitzender des Bundesverbands Mergers & Acquisitions