Cyber-Crime: Existenzielle Bedrohung des Unternehmensvermögens

Von Niklas Gretser und Alexander Wagner

Niklas Gretser

Alexander Wagner

Der anhaltende Trend zur Digitalisierung verändert auch das Umfeld für Kriminelle. In einer unglaublichen Geschwindigkeit haben sich die Täter an neue Gegebenheiten angepasst und digitalisieren ihre Tatwerkzeuge und die Tatbegehungsweisen. Die Digitalisierung der Kriminalität verschafft auch der sog. Underground Economy starkes Umsatzwachstum. War es in der Vergangenheit eher ein kleiner Täterkreis, der über das Spezial-Know-how verfügte, IT-Systeme zu „hacken" oder anderweitig IT für kriminelle Handlungen einzusetzen, so kann sich heute praktisch jeder Täter Wissen anhand von frei zugänglichen Tutorials aneignen und auch diverse Produkte und Dienstleistungen auf anonymen Marktplätzen im Netz dazukaufen. Mit Bitcoin & Co. haben sich „sichere" digitale Zahlungswege und auch eine perfekte Infrastruktur zur anonymen Abwicklung illegaler Geschäfte entwickelt.

Schwachstelle Mensch

Nach allem was bekannt ist, sind die Mehrzahl der Cyber-Angriffe von außen ungezielte Breitenangriffe z.B. auf Sicherheitslücken in weitverbreiteten Betriebssystemen. Die Wahrscheinlichkeit ist hoch, dass Kriminelle auch in Zukunft verstärkt versuchen werden, mit weiterentwickelter Schadsoftware Geld von Unternehmen zu erpressen. Gezielte Angriffe dagegen sind aufwendig für die Täter, kommen weniger häufig vor, können aber die Betroffenen enorm schädigen. Neben „Hacking" und DDoS-Attacken (Distributed-Denial-of-Service) haben sich Tätergruppen darauf spezialisiert, mittels gestohlener Identitäten, ausgespähter Mail-Accounts und unter Anwendung von Social Engineering erfolgreiche Angriffe auf Unternehmen und ihre Vermögen zu fahren. In vielen Fällen wird dabei gezielt die Schwachstelle „Mensch" ausgenutzt, indem Mitarbeiter von Unternehmen durch Täter entweder gezielt angeworben oder eher unwissentlich zum „Komplizen" gemacht werden.

CEO-Fraud ist in diesem Zusammenhang inzwischen ein eher bekanntes Tatmuster. Trotzdem gelingt es den Betrügern weiterhin, durch Abwandlungen und Weiterentwicklungen dieses Betrugsmusters insbesondere mittelständischen Unternehmen massive Schäden zuzufügen. Die Varianten und Gelegenheiten sind vielschichtig: Mittels „Phishingattacken" werden Passwörter von E-Mail-Postfächern abgegriffen oder mit Schadsoftware (z.B. über „Keylogger") die Hardware infiziert, sämtliche Eingaben über die Tastatur des betroffenen Rechners mitgelesen und somit unternehmensinterne Informationen gewonnen, die im Anschluss gezielt für Straftaten genutzt werden. Aus unserer Praxis kennen wir Fälle, bei denen E-Mails zu bevorstehenden hohen Investitionen von Unternehmen durch die Täter mitgelesen wurden und das Wissen mit hoher krimineller Energie dafür genutzt wurde, um die mit diesen Investitionen verbundenen Zahlungen auf Konten im Netzwerk der Betrüger umzuleiten. Das können z.B.

Zahlungen in Verbindung mit M&A-Transaktionen oder Kapitalanlagen sein. In einem Fall haben Täter erfolgreich betrogen, indem die Ausschüttung einer Kapitalanlage an einen langjährigen Investor umgeleitet worden war.

Die professionellen Täter verschleiern in solchen Fällen geschickt die Ausübung der Tat und im Anschluss auch ihre Spuren. Die Aufklärung ist oft enorm schwer, weil die Angreifer regelmäßig sog. Proxy-Server oder durch Schadsoftware fremdgesteuerte (Firmen-)Server nutzen. Das heißt, die digitale zurückverfolgte Spur verliert sich in der Praxis bei einem Proxy-Dienstleister oder bei einem unbeteiligten Dritten. Beide haben aber in vielen Fällen selbst mit der Tat oder dem Täter nichts zu tun.

Natürlich ist der Umstand kritisch, dass insbesondere die Anbieter solcher Proxy-Services regelmäßig im Ausland sitzen und erfahrungsgemäß keine Anfragen der geschädigten Unternehmen beantworten. Auch staatsanwaltliche Ermittlungen verlaufen oft nicht erfolgversprechend, was auch damit zusammenhängt, dass professionelle Täter mehrere Proxy-Server hintereinanderschalten und so mehrere Schichten (Layer) der Verschleierung nutzen.

Wettlauf gegen die Zeit

Die internationalen Ermittlungen sind grundsätzlich ein Wettlauf gegen die Zeit! Es besteht die Gefahr, dass nationale Speicherfristen schneller verstreichen als die internationale Zusammenarbeit von Strafverfolgungsbehörden organisiert werden kann. Das Geld aus der Straftat ist dann in den meisten Fällen bereits über internationale Kanäle bestmöglich verschleiert und in den Verfügungsbereich des Täters transferiert worden.

Das Entdeckungsrisiko für Straftäter ist in diesen Fällen also vergleichsweise gering. Anonymisierung und Kryptierung verhindern in weiten Teilen die Beweissicherung und das Internet wird zwar nicht zum rechtsfreien, aber infolge der funktionalen und territorialen Grenzen des Strafrechts, weitgehend zum strafverfolgungsfreien Raum. Die psychologische Hemmschwelle wird wohl zusätzlich niedriger, weil es in der Regel nicht zu einem persönlichen Täter-Opferkontakt kommt.

Aber auch immaterielle Vermögenswerte von Unternehmen werden Ziel von kriminellen Angriffen. In diesem Zusammenhang stellt sich sehr häufig die Frage, ob der Täter ein Mitarbeiter war. Zum Beispiel wurde in einem Fall ein erfolgreicher Webshop „kopiert“. Offensichtlich hatte ein ehemaliger Mitarbeiter auf dieser Basis selbst eine Online-Handelsplattform aufgebaut. Das Unternehmen verlor Marktanteile, der Imageschaden war enorm. In anderen Fällen wurden wertvolle Daten aus dem Bereich Forschung und Entwicklung entwendet. Das Unternehmensnetzwerk war zwar gegen Angriffe von außen gut geschützt, dass Berechtigungskonzept intern war allerdings mangelhaft, so dass der Datendiebstahl lange unbemerkt bleiben konnte. Auch wenn die Wahrscheinlichkeit hoch war, dass es sich um einen Innentäter – also Mitarbeiter – gehandelt haben muss, war die Identifizierung des Täters nicht mehr möglich, da keine Logfiles zu Aktivitäten und Zugriffen auf den relevanten Servern vorhanden waren.

> Das Internet wird weitgehend zum strafverfolgungsfreien Raum.

Funktionalität versus Sicherheit

Die Chancen der Täter liegen hier in einer gewissen Unbedarftheit und auch in dem Dilemma, dass eine funktionale Arbeitsumgebung auch zu Kompromissen in der IT-Sicherheit führen kann, wie zum Beispiel bei modernen Arbeitsplatzkonzepten mit „bring-your-own-device“, oder zu Ineffizienzen bei der Sperrung von externen Ports.

Auch die Überforderung der Nutzer mit zunehmender Komplexität von Systemlandschaften

und der Anzahl vernetzter smarter Elektronik in allen möglichen Lebensbereichen führt zu Sicherheitslücken. Diese zu schließen, ist nach wie vor ein Katz-und-Maus-Spiel. Und was bei allen Anstrengungen zur Aufrüstung von IT-Sicherheit technisch nicht oder nur unzureichend gelöst werden kann, ist die Verwundbarkeit des „Menschen" bzw. Mitarbeiters im Unternehmen und die mit Kriminalitätsrisiken behafteten digitalisierten Geschäftsmodelle.

Bitte beachten Sie die folgenden wichtigen Empfehlungen:

- Führen Sie regelmäßig Schulungen der Mitarbeiter durch und sensibilisieren Sie die Mitarbeiter hinsichtlich der Gefahren und der betrügerischen Handlungsmuster.
- Beachten Sie die Empfehlungen und News z. B. des BSI zur IT-Sicherheit.
- Ändern Sie regelmäßig Passwörter, verwenden Sie insbesondere keine Werkseinstellungen.
- Prüfen Sie die Sicherheit Ihrer Backup-Server und stellen Sie sicher, dass Backups offline an einem sicheren Ort verwahrt werden.
- Erstellen und aktualisieren Sie Berechtigungskonzepte für den Datenzugriff.
- Prüfen Sie, wie Zugriffe auf sensible Daten sicher aufgezeichnet werden können.
- Überdenken Sie die dienstlichen und privaten Veröffentlichungen von (temporären) Informationen in sozialen Netzwerken.
- Achtung vor Phishing-Attacken! Öffnen Sie keine Attachements und Links, wenn Sie den Absender nicht kennen.
- Überprüfen Sie Absender-E-Mailadressen (minimale Abweichungen, Ansicht vollständiger Adressen etc.).
- Nehmen Sie eine kritische Grundhaltung ein, bei Zahlungsanweisungen per Mail und Telefon generell, in Verbindung mit Abweichungen vom Sollprozess im besonderen Maße.
- Lassen Sie sich Weisungen auf anderem Weg intern bestätigen, auch wenn Verschwiegenheit gefordert wird. Ggf. schaffen Sie einen gesonderten Meldeweg bei derartigen Fällen.

Alexander Wagner war u. a. Bediensteter des Landeskriminalamts NRW und verantwortet als Partner den Bereich Fraud Investigations und IT Forensic im Competence Center Fraud / Risk / Compliance von Baker Tilly.

Niklas Gretser war u. a. Kommissar der Polizei Niedersachsen im Bereich Cybercrime und Wirtschaftskriminalität und ist im Competence Center Fraud / Risk / Compliance von Baker Tilly Experte für Fraud Investigations, Cyber Crime und IT Forensic.