Foto: John Lund/getty images

„JE KOMPLEXER DIE IT-INFRASTRUKTUR, DESTO SCHWIERIGER IST ES, DIESE ABZUSICHERN“

Cyber-Angriffe auf IT-Systeme von Unternehmen und Organisationen haben drastisch zugenommen. Lässt sich Sicherheit für die gesamte IT-Landschaft eines Unternehmens überhaupt noch garantieren? Und welche Möglichkeiten gibt es, das komplexe Thema IT-Sicherheit zu vereinfachen? HaysWorld hat sich dazu mit dem Chief Information Security Officer der Deutschen Bank Al Tarasiuk unterhalten.

Das Interview führte Frank Schabel

Man liest sehr viel über Cyber-Angriffe auf der ganzen Welt. Stellen solche Angriffe eine echte Bedrohung dar oder ist das ein Hype-Thema?

Das ist kein Hype, sondern eine echte Gefahr. Die Angreifer – zu denen kriminelle Gruppen, Hacktivisten oder auch Regierungen gehören – gehen äußerst kreativ vor. Sie haben unterschiedliche Beweggründe für ihre Handlungen und die Auswahl der Ziele. Manche sind politisch oder finanziell motiviert, andere hingegen möchten gezielt Schaden verursachen. Doch die von diesen Angriffen ausgehende Bedrohung ist in allen Fällen sehr real. Deshalb nehmen wir das auch sehr ernst.

Wie schützt sich die Deutsche Bank vor Cyber-Angriffen? Werden proaktive oder reaktive Maßnahmen eingesetzt?

Im Idealfall sollte jedes Unternehmen proaktiv agieren. Es müssen die richtigen Kontrollen vorhanden sein, mit denen Angriffe erkannt und verhindert werden können und darauf reagiert werden kann. Die Schwierigkeit besteht darin, dass die Angreifer immer versuchen werden, einen Schritt voraus zu sein. Man darf nie nachlässig werden und ist gut beraten, mehrstufige Sicherheitsmaßnahmen aufzubauen. Wir sprechen in diesem Zusammenhang von einem „gestaffelten Verteidigungskonzept“.

Wie gehen die Angreifer vor?

Normalerweise beobachten die Angreifer einen zunächst, um herauszufinden, wo es Schwachstellen gibt. Anschließend nutzen sie diese Informationen, um festzulegen, wie der Angriff auf diese Schwachstelle ausgeführt werden soll. Es sind mehrere Schritte, die auch als „Cyber Kill Chain“ bezeichnet werden.

Was kann man dagegen unternehmen?

Man muss die Bedrohungen so früh wie möglich erkennen – denn je früher sie erkannt werden, desto weniger Schaden können sie anrichten.

Klingt plausibel …

Ja, allerdings gehen die Angreifer sehr geschickt vor und bringen – je nach Motiv – sehr viel Zeit und Mühe auf, eine Organisation zu infiltrieren. Aber wenn es keine einfache Einbruchsmöglichkeit gibt, ziehen viele Angreifer wieder weiter und suchen sich ein anderes Ziel. Schaut man sich einmal an, wo sie Schwachstellen ausnutzen, sind es die einfachen. Diejenigen, auf die die Unternehmen nicht achten.

Foto: Deutsche Bank AG

Al Tarasiuk

Al Tarasiuk ist seit Mai 2015 als Head of Information Technology (IT) Security bei der Deutschen Bank tätig und wurde im Januar 2016 zum Group Chief Information Security Officer ernannt.

Zuvor hatte er im Office of the Director of National Intelligence, einem nachrichtendienstlichen Teil der US-Regierung, als United States Intelligence Community Chief Information Officer (CIO) gearbeitet. In diese Position wurde er im Februar 2011 vom damaligen Präsidenten Barack Obama berufen. In seinen Verantwortungsbereich fielen unter anderem Informationssicherheit, IT-Architektur und -Strategie sowie Informationsmanagement.

Davor war Al Tarasiuk 23 Jahre in unterschiedlichen IT-Positionen beim US-Geheimdienst tätig und stieg anschließend zum CIO auf. Seine berufliche Laufbahn begann er als Projektingenieur bei Radio Free Europe und Radio Liberty. Al Tarasiuk schloss sein Studium als Bachelor of Science in Elektrotechnik am New Jersey Institute of Technology ab und machte seinen Diplomabschluss in Betriebstechnik an der George Washington University.

Wie schnell muss eine Reaktion erfolgen?

Die frühzeitige Erkennung spielt eine sehr zentrale Rolle. Deshalb ist eine kontinuierliche Überwachung so wichtig. Eines der neuen Konzepte, die wir umsetzen, basiert auf der sogenannten Threat Intelligence. Das bedeutet, die Bedrohungslandschaft zu verstehen und zu wissen, wie Angreifer ihre Strategien für Angriffe auf eine Branche anpassen. Um von diesem Ansatz bestmöglich zu profitieren, muss man Zugriff auf ein Netzwerk mit umfangreichen Sicherheitsinformationen haben. Ein Beispiel dafür sind Dienstleistungen von Unternehmen, die das Internet überwachen und Informationen bereitstellen, mit denen man seine internen Konzepte entsprechend anpassen kann.

Ist es vor diesem Hintergrund überhaupt möglich, Sicherheit für die gesamte IT-Landschaft zu gewährleisten?

Die Herausforderung dabei ist, dass sich die Bedrohungslandschaft ständig verändert. Man muss immer auf der Hut sein und sich auf die Aufrechterhaltung der „IT-Hygiene“ konzentrieren. Zudem muss man verstehen, wie die Organisation mit der Außenwelt interagiert, seine Vermögenswerte im Blick behalten und dann Schritt halten mit den technologischen Entwicklungen. Das Internet wurde nie mit einem Sicherheitsmodell aufgebaut. Nahezu alle Technologien wurden von den Angreifern bereits ins Visier genommen, die genau wissen, wo die Schwachstellen zu finden sind. Um unerkannt zu bleiben, verändern die Angreifer ständig ihre Taktiken und Malware. Deshalb sind mehrstufige Sicherheitsmaßnahmen erforderlich, denn es ist nicht immer möglich, die vielen unterschiedlichen Varianten von Malware zu erkennen – insbesondere, wenn diese Malware von besonders raffinierten Angreifern kommt. Deshalb wird es im Grunde nie eine vollkommene Sicherheit geben. Ein ganzheitlicher Ansatz mit frühzeitiger Erkennung ist eine der besten Möglichkeiten, sich zu schützen und die Angreifer so früh wie möglich aufzuhalten.

> „Da das Thema Cyber-Sicherheit relativ neu ist, ist es zudem alles andere als einfach, erfahrene Praktiker in diesem Bereich zu finden.“

Gibt es irgendwelche Methoden oder Lösungen, um das komplexe Thema IT-Sicherheit zu vereinfachen?

Besonders in großen, weltweit agierenden Organisationen besteht die Vereinfachung der Sicherheit darin, die IT-Landschaft zu vereinfachen. Je komplexer die Infrastruktur, desto schwieriger ist es, diese abzusichern. Neben Kostensenkungen konzentrieren sich zahlreiche Unternehmen zunehmend darauf, ihre technologische Infrastruktur zu konsolidieren, um diese zu vereinfachen und besser schützen zu können. Außerdem ist es wichtig, eine robuste Sicherheitsarchitektur sowie einen Sicherheitsrahmen einzuführen. Hat man das nicht, läuft man Gefahr, Sicherheit mit Ad-hoc-Maßnahmen aufzubauen, und hat am Ende Sicherheitstechnologien, die nicht zusammenpassen. Sie können zwar ein spezifisches Problem lösen, bieten jedoch keine Abhilfe bei größeren Themen.

Trägt aus organisatorischer Sicht eine bestimmte Abteilung die Verantwortung für die Cyber-Sicherheit oder ist das ein Thema, für das alle Abteilungen und alle Mitarbeiter verantwortlich sind?

Ich bin fest davon überzeugt, dass man eine zentrale Abteilung benötigt, die sich um die Programm- und Umsetzungsplanung kümmert und die sicherstellt, dass wichtige Richtlinien und Standards eingeführt werden. Aber ich bin ebenso davon überzeugt, dass sich auch die Mitarbeiter in den Geschäftsbereichen dafür einsetzen müssen, diese Richtlinien anzuwenden. Es ist also beides wichtig, sowohl der zentralisierte als auch der dezentralisierte bzw. hybride Ansatz. Mit einer separaten Abteilung, die sich allein um das Thema kümmert, kommt man nicht weiter. Es muss als integraler Bestandteil des Unternehmens angesehen werden.

Rechnen Sie mit einem höheren Bedarf an Spezialisten im Bereich IT-Sicherheit?

In jedem Fall. Weil man jetzt die Bedrohung über alle Branchen hinweg und nach all den Sicherheitsvorfällen erkannt hat, suchen nun alle nach denselben Talenten in diesem Bereich. Die akademischen Strukturen in den Ländern kommen der wachsenden Nachfrage nach solchen Spezialisten allerdings nicht nach. Da das Thema Cyber-Sicherheit relativ neu ist, ist es zudem alles andere als einfach, erfahrene Praktiker in diesem Bereich zu finden. Dieser Engpass wird uns noch eine ganze Weile begleiten, aber ich sehe auch als positive Entwicklungen, dass die Lehre mehr und mehr Studiengänge einführt, um Personal gut auszubilden.

Was ist Ihrer Meinung nach das nächste große Thema im Bereich Cyber-Sicherheit?

Das Internet der Dinge. Jeder spricht darüber, doch die wenigsten berücksichtigen die Sicherheit all dieser Geräte. Kameras und sogar Kühlschränke werden zunehmend mit internetfähigen Computern ausgestattet. All diese Geräte haben dann ihre eigenen IP-Adressen und werden zum Ziel von Angreifern oder können in Botnet-Attacken eingesetzt werden. Meiner Ansicht nach ist das eine große Herausforderung. Eine weitere Gefahr besteht darin, dass sich die Angreifer weltweit immer stärker virtuell vernetzen. Nicht, dass sie physisch an einem Ort zusammensitzen. Sie kennen sich vielleicht nicht einmal. Aber sie kommen virtuell zusammen und nehmen sich ein gemeinsames Ziel vor. Wie man sich dagegen schützen kann? Ich möchte nicht den Eindruck erwecken, es gebe keine Hoffnung. Ich bin nach wie vor davon überzeugt, dass sich ein Unternehmen schützen kann, wenn es über ein robustes, ganzheitliches Informationssicherheitsprogramm verfügt, mit dem alle Vorgänge vom Anfang bis zum Ende im Hinblick auf Mitarbeiter, Prozesse, Technologie und Richtlinien beleuchtet werden. Ist das nicht der Fall, kann man sich schnell Probleme einhandeln.