TIBER-DE-Tests: Deutschlands Banken sollen widerstandsfähiger werden

Von Miriam Veith – Fast jeder Internetuser wurde schon einmal mit Cyberkriminalität konfrontiert. Da Banken zu den kritischen Infrastrukturen gehören, kurz KRITIS, und daher über sensible Daten wie Namen, Kontoverbindungen oder Passwörter ihrer Kunden verfügen, sind sie besonders attraktiv für Hacker und deren Cyberattacken. Diese versuchen aus aller Welt die IT-Systeme der Institute zu überlisten, um an Daten zu gelangen, die für sie bares Geld bedeuten können. Die Zahl der Cyberattacken nimmt im Zuge der Digitalisierung kontinuierlich zu. Laut dem Branchenverband Bitkom ist in Deutschland innerhalb der letzten zwei Jahre eine Schadenshöhe von 100 Milliarden Euro entstanden. Emotet gilt dabei als die weltweit gefährlichste Schadsoftware, die in der Lage ist, beispielsweise E-Mails auszuspähen.

Da professionelle Hacker heutzutage zum Teil sogar mit Geheimdiensten mithalten können, entstehen stetig neue Bedrohungen. Das Finanzwesen hat sich aber in den letzten Jahren durchaus als resistent gegenüber Cyberattacken erwiesen, was darauf zurückzuführen ist, dass gerade in diesem Sektor sehr viel investiert wird. Vor allem in neue Technik zur Abwehr, aber auch durch gezielte Schulungen der Mitarbeiter. Letztlich birgt die menschliche Komponente aber immer noch das höchste Risiko und somit enormes Potenzial für Angriffe, aufgrund von Unwissen oder leichtfertigem Umgang, weshalb gerade dort Hacker versuchen, Schlupflöcher zu identifizieren.

Initiative der Europäischen Zentralbank

Banken sind gezwungen, ihre Abwehrsysteme immerzu nachzurüsten und auf die sogenannte Cyberresilienz, also die Widerstandsfähigkeit gegenüber Cyberattacken, zu überprüfen. Für die Analyse, wo Implementierungsfehler oder menschliche Schwächen liegen, gibt es verschiedene Penetrationstests, die bekannte Schwachstellen unter die Lupe nehmen. Die klassischen Tests beschränken sich dabei auf die technologische Ebene des IT-Systems. Es gibt aber auch die Möglichkeit, mittels TIBER-Tests (Threat Intelligence-based Ethical Red-Teaming) einen realitätsnahen Cyberangriff zu simulieren, um eine Bedrohungsanalyse unter kontrollierten Bedingungen durchzuführen. Dieses Verfahren bezieht neben der technischen Komponente auch menschliche Faktoren mit ein.

Basierend auf diesem Ansatz hat die EZB eine europäische Rahmenvorgabe namens TIBER-EU entwickelt, um die Cyberresilienz europäischer Banken zu stärken sowie Prozesse in diesem Bereich zu harmonisieren. Länder wie Belgien oder die Niederlande und deren Erfahrungen mit TIBER-EU sollen nun als Inspiration für eine nationale Implementierung von TIBER-DE dienen. Ein Lenkungsausschuss der Deutschen Bundesbank und der BaFin will noch im Jahr 2020 das Rahmenwerk auf den Weg bringen.

Das TIBER Cyber Team (TCT), ein nationales Kompetenzteam, welches zur Bundesbank gehört, stellt die Kommunikationsschnittstelle nach außen dar, begleitet die Unternehmen während des gesamten Testverlaufs und überprüft die Einhaltung der Rahmenbedingungen. Die Anwendung der Tests soll auf freiwilliger Basis erfolgen, somit stellen diese kein bankenaufsichtliches Instrument dar.

Der TIBER-DE-Test ist in drei Phasen untergliedert und dauert in der Regel mehrere Monate an, auch eine weitere optionale Phase kann in das Testverfahren eingebunden werden. Die Analyse der allgemeinen Bedrohungslage stellt hierbei die optionale Testphase dar, die die potenziellen Bedrohungen für das Finanzwesen in einem Lagebild zusammenfasst. Ausgehend hiervon wird die erste der drei Haupttestphasen eingeleitet, die Vorbereitungsphase, in welcher die gesamte Planung und Beauftragung in- wie extern vorgenommen wird. Die Geschäftsleitung des Unternehmens wählt eine intern verantwortliche Instanz für die Durchführung des Tests aus, das sogenannte White Team. Sonst darf niemand auf interner Ebene informiert werden, um eine realitätsnahe Umgebung für simulierte Attacken zu generieren und somit die kritischen Funktionen des Unternehmens überprüfen zu können. Entsprechend ausgeschlossen von diesem Wissen wird das Blue Team, welches hausintern für die IT-Sicherheit zuständig ist.

Überprüfung der Strukturen durch ethische Hacker

Das White Team definiert die Ziele sowie Rahmenbedingungen des Tests in Absprache mit der Geschäftsleitung und dem TIBER Test Manager (TTM), der aus dem TCT als Ansprechpartner für das Unternehmen bestellt wird. Die BaFin wird ebenfalls informiert. Da das Testverfahren eigens produzierte Risiken oder Systemausfälle nach sich ziehen kann, nimmt das White Team eine Risikobewertung vor und etabliert Risikomanagementkontrollen. Zudem werden externe Dienstleister beauftragt, das Unternehmen im Rahmen des TIBER-Tests unter kontrollierten Bedingungen anzugreifen. Diese beiden Teams werden Red Team sowie Threat Intelligence Team (TIT) genannt.

Das TIT leitet die eigentliche Testphase mit der Informationsbeschaffung für das Red Team ein. Falls das Unternehmen die optionale Phase umgesetzt und somit ein Lagebild generiert hat, kann das TIT dieses in den eigenen Bericht mit aufnehmen. Nach der Instruktion durch das TIT entwickelt das Red Team Angriffsstrategien und Szenarien. Diese zielen, wie bereits erwähnt, auf die kritischen Funktionen sowie Prozesse und organisatori-

schen Strukturen des Unternehmens ab. Unter Aufsicht des Risikomanagements und somit im engen Austausch mit dem White Team führt das Red Team regelmäßig Attacken auf das IT-System des Unternehmens durch. Die Testfortschritte werden dabei im wöchentlichen Zyklus dem TTM übermittelt.

In der letzten Phase des TIBER-Tests werden die Erkenntnisse aus den Angriffen des Red Teams analysiert und in einem Report zusammengefasst. Bei einem gemeinsamen Feedbacktreffen, an welchem alle Beteiligten des TIBER-Tests teilnehmen, werden das Vorgehen des Red Teams und die Ergebnisse der Angriffe präsentiert. Außerdem werden Maßnahmen festgelegt, die das Unternehmen zugunsten einer gesteigerten Cyberresilienz umsetzen soll. Die BaFin und Bundesbank diskutieren aktuell auch noch über den Einsatz eines Purple Teams, das den Austausch zwischen Red Team und Blue Team fördern soll.

Das TIBER-DE-Testverfahren stellt ein geeignetes Instrument dar, um allgemein die IT-Sicherheit zu stärken. Das zeigen auch erste Erfahrungen mit TIBER-NL aus den Niederlanden. Ursprünglich sollten TIBER-Tests nur im Finanzwesen durchgeführt werden, allerdings wurde das Projekt mittlerweile ausgeweitet und beispielsweise in Versicherungsunternehmen erfolgreich angewandt. Zudem sind verschiedene TIBER-Netzwerke entstanden, in welchen sich Unternehmen, die bereits Erfahrungen mit TIBER-Tests gesammelt haben, austauschen können. Daran wollen Bundesbank und BaFin mit TIBER-DE anknüpfen.

„Die Wahrscheinlichkeit, Opfer einer Cyberattacke zu werden, ist höher als je zuvor“

Herr Sauer, das Finanzwesen wird allgemein den „KRITIS“, also den kritischen Infrastrukturen, zugeordnet. Was ist darunter konkret zu verstehen?

Kritische Infrastrukturen im Sinne des BSI-Gesetzes sind Einrichtungen, die verschiedenen Sektoren, beispielweise Energie, Informationstechnik, Telekommunikation, Transport und Ernährung, aber auch Finanz- und Versicherungswesen angehören. Sie sind von hoher Bedeutung für das Funktionieren des Gemeinwesens, denn durch ihren Ausfall oder ihre Beeinträchtigung würden erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit in Deutschland eintreten.

Daten sind die neue Währung des 21. Jahrhunderts. Aber was genau machen Hacker mit diesen und wie wird Profit aus dem Angriff geschlagen?

Ich würde behaupten, dass man personenbezogene Daten als das Öl oder vielleicht sogar als das Gold des Werbemarktes bezeichnen kann. Das Ziel der Werbeproduzenten ist, ihre Produkte möglichst zielgenau an diejenigen Kunden zu bringen, die sich für die Angebote interessieren. Entweder wird dafür auf das Wissen über diese Personen zurückgegriffen oder es werden mögliche Kunden in Gruppen mit ähnlichen Eigenschaften einsortiert und anschließend davon ausgegangen, dass sie ähnliche Kaufentscheidungen treffen.

Der weltweite Markt mit mehr als 1000 Datensammlern und -händlern beinhaltet sowohl namenhafte Unternehmen wie Facebook oder Google, aber auch öffentlich eher unbekannte Firmen. Alle von ihnen durchforsten soziale Netzwerke, analysieren das Online-Verhalten der Nutzer oder handeln mit persönlichen Daten. Der Verkauf sogenannter „Endkunden-Daten“ ist natürlich auch für die Hacker ein sehr interessantes, einfaches Geschäftsmodell.

Was können Institute tun, um sich vor Schäden durch bekannte Angreifer wie Emotet zu schützen?

Es gibt verschiedene Möglichkeiten um sich und seine Daten zu schützen. Zuallererst sollte man möglichst zeitnah die bereitgestellten Sicherheitsupdates installieren und regelmäßige Backups zum Schutz der Daten machen. Außerdem halte ich es für sinnvoll, eine Antiviren-Software zu installieren und ein gesondertes Benutzerkonto auf dem Computer einzurichten. Dort kann man surfen oder E-Mails schreiben. Aber auch dabei ist Vorsicht geboten, denn viele Hacker nutzen E-Mails, um Viren oder Ähnliches zu versenden. Daher sollte man auch bei vermeintlich bekannten Absendern enthaltene Links zuerst überprüfen und bei einer verdächtigen E-Mail den Absender anrufen, um sich nach der Glaubhaftigkeit des Inhalts zu erkundigen. Diese Maßnahmen müssen sogar laut BSI innerhalb der IT-Infrastruktur umgesetzt werden.

Ingo Sauer

Certified Information Security Manager (CISM, CSP), CMO, Auxilium Cyber Security GmbH, Ettlingen

Aber wie kann es dann sein, dass Hacker trotz Aufklärung der Mitarbeiter und Vorsichtsmaßnahmen, wie beispielsweise Firewalls, immer wieder erfolgreich in Systeme eindringen?

Zu ihrer Frage fällt mir ein gutes Zitat des amerikanischen Programmierers Richard Stallman ein: „Hacken bedeutet, die Grenzen des Möglichen auszutesten, im Geiste verspielter Cleverness." Damit meint er, dass es sich oft um ein schwieriges Unterfangen handelt, denn Hacks sind sehr vielschichtig. Das Bild, dass die meisten von uns aus Filmen kennen, wenn Hacker für ein paar Sekunden auf die Tastatur tippen, entspricht nicht annähernd der Realität. Oft steckt hinter einem erfolgreichen Hack tage- oder sogar wochenlange Detailarbeit. Während die meisten Hacker früher oftmals alleine im Cyberspace unterwegs waren, sind es heute gut organisierte Gruppen mit technisch erfahrenen Mitarbeitern, die für Bezahlung in ein System vordringen.

Dabei muss man sagen, dass es immer irgendeine Möglichkeit des Eindringens gibt, denn kein System kann eine hundertprozentige Sicherheit gewährleisten. Letztendlich spricht man bei diesen Cyberattacken von sogenannten „Advanced Persistent Threats", oder kurz APTs. Auf Deutsch bedeutet das in etwa: „fortgeschrittene andauernde Bedrohung". Diese APTs sind oft komplexe und zielgerichtete Angriffe auf vertrauliche Daten von Behörden, aber auch auf Groß- und Mittelstandsunternehmen aller möglicher Branchen.

Die immer wichtiger werdende Rolle des Menschen sollte man dabei nicht vernachlässigen: Ein guter Hacker versteht nicht nur Computersysteme, er kann auch Menschen verführen, ihm Informationen zu verraten. Einer der ältesten Tricks bei Internetbetrügereien ist deshalb das Social Engineering.

Wollen Sie damit sagen, dass der Faktor Mensch immer noch das größte Risiko für die IT-Sicherheit darstellt? Was können Banken tun, um diese Gefahr zu minimieren?

Ja, genau, daher ist heutzutage der erste Schritt mehr denn je der wichtigste. Die Mitarbeiter müssen sich im Unternehmen und mit ihrer Arbeit wohlfühlen. Das klingt vielleicht einfach, ist es aber leider nicht. Man kann es nie allen recht machen und somit ist jemand auch mal verstimmt. Kommen dann noch private Sorgen hinzu, sinkt oft die Hemmschwelle für einen Firmenwechsel oder es werden gegen Bezahlung firmeninterne Daten herausgegeben. Bisher haben viele Banken versucht mithilfe technischer Lösungen wie „Data Loss Prevention", kurz DLP, einen Schutzschirm um wertvolle Informationen zu legen. Aber Menschen sind sehr erfinderisch. Die immer höheren Mauern nützen leider nichts, wenn der „Spion" bereits drin ist!

„Es gibt immer die Möglichkeit einzudringen, kein System kann hundertprozentig sicher sein."

„Oft steckt hinter einem Hack wochenlange Detailarbeit."

Eine bewährte Gegenmaßnahme ist die Aufklärung und Schulung von Mitarbeitern in dem Themenbereich Compliance. Also dem sorgsamen und sicheren beziehungsweise vertrauensvollen Umgang mit Daten und schützenswerten Firmeninformationen. Aktuell gibt es auch bereits technische Lösungen, welche auf Benutzer-Verhaltensanalyse fungieren. Doch diese werden häufig in anderen Ländern auch außerhalb der EU eingesetzt, da sie in Deutschland nur schwer eingeführt werden können.

Innerhalb der letzten zwei Jahre wurden etwa 114 Millionen neue Schadprogramm-Varianten entdeckt, die potenziellen Bedrohungen nehmen also zu. Inwieweit hat das etwas mit der Digitalisierung zu tun?

Sehr viel sogar. Zwar profitieren wir alle von den vielen Vorteilen einer zunehmend digitalisierten und vernetzten Welt, aber das hat auch einen hohen Preis: Cyberangriffe sind zu einer ernsthaften Bedrohung geworden. Sie betreffen nicht nur unsere Daten, sondern unser alltägliches Leben. Daher sind in jeder Organisation umfassende Sicherheitsmechanismen und sicherheitsorientiertes Denken unerlässlich.

Haben Sie persönlich den Eindruck, dass der Finanzplatz Deutschland gegen Cyberangriffe gewappnet ist?

Im Grunde genommen bin ich mir sicher, dass wir hier in Deutschland ganz gut gewappnet sind. Allerdings sind uns allen leider die Hacker immer einen Schritt voraus und wir müssen uns mehr denn je anstrengen. Gerade im Bereich der „intelligenten" Angriffe, durch den Einsatz neuer Technologien, sind uns die „Bösen" voraus.

In einigen Ländern, darunter Belgien oder die Niederlande, wurden sogenannte „TIBER-EU-Tests" erfolgreich umgesetzt, um die Cyberabwehrfähigkeit von Banken zu prüfen. Nun sollen nach diesem Vorbild „TIBER-DE-Tests" in Deutschland zum Einsatz kommen. Was unterscheidet dieses Verfahren von den klassischen Penetrationstests?

Der „Red-Teaming-Ansatz", wie ihn das TIBER-DE-Framework vorsieht, geht über das klassische Pentesting hinaus. So be-

rücksichtigt Red Teaming neben technischen vor allem auch menschliche Sicherheitsfaktoren.

Der Tester stellt also nicht nur Systeme innerhalb einer Umgebung auf den Prüfstand, sondern auch die Menschen und die Prozesse im Unternehmen. Erst dadurch ergibt sich ein umfassendes Bild der aktuellen Sicherheitslage, welches dem Unternehmen ermöglicht, sich optimal auf Angriffe vorzubereiten.

Welche Art von Penetrationstest führen Sie mit Ihren Kunden durch und was sind für Sie charakteristische Fehlerquellen, die diese Tests aufdecken?

Wir sind in der Lage, Test- und Codeüberprüfungsszenarien für Produkte durchzuführen, die von benutzerdefinierten Webanwendungen und Linux-basierten Systemen bis hin zu internen und externen Netzwerkpenetrationstests reichen. Darauf aufbauend erstellen wir einen umfassenden Bericht mit Ergebnissen und Empfehlungen, um Schwachstellen zu beseitigen.

Viele von uns sind aufgrund der aktuellen Corona-Pandemie dazu gezwungen, im Homeoffice zu arbeiten. Ist das nicht ein weiteres Sicherheitsrisiko und denken Sie, dass die Zahl von Cyberattacken dadurch zunimmt?

Es ist durchaus so, dass sich einige Menschen besonders im Homeoffice nur unzureichend vor Cyberattacken schützen. Viele sind verunsichert und mit der Ausnahmesituation überfordert. Allerdings sollte sich kein IT-Verantwortlicher beirren lassen. Das wichtigste ist, die übliche Cyberhygiene weiterzuführen. Beispielsweise ist es wichtig, seine wichtigsten Konten zu beschränken oder zu schützen. IT-Experten sollten ihre User regelmäßig über Phishingangriffe informieren und sie darauf hinweisen, dass starke Passwörter sehr wichtig sind. Die regelmäßige Kontrolle der USB-Geräte und die Entfernung veralteter Software spielen eine ebenso große Rolle.

Auch regelmäßige Backups sind in diesem Zusammenhang notwendig, um im schlimmsten Falle die wichtigsten Daten wiederherstellen zu können. Die IT-Experten sollten im gesamten Netzwerkverkehr auf Auffälligkeiten achten und potenzielle Risiken identifizieren.

Auch Banken wurden in den letzten Wochen häufig Opfer von Betrugsfällen wie beispielsweise Fakeseiten, die die eigene offizielle Homepage imitieren. Gibt es gewisse Merkmale, auf die die Nutzer achten können, um falsche Seiten zu identifizieren?

Cyberkriminelle tarnen ihre Fakeseiten oft sehr gut, insbesondere wenn sie bekannte Online-Shops imitieren. Den meisten von uns fällt auf den ersten Blick gar nicht auf, dass es sich nicht um die Originalseite handelt. Aber es gibt einige Anzeichen, die helfen, eine seriöse Seite von einem Fakeshop zu unterscheiden. Zum einen sollte man skeptisch werden, falls die eigentlich bekannte Webadresse Ungereimtheiten aufweist oder überhaupt nicht zum Inhalt der Seite passt. Darüber hinaus locken Fakeshops ihre Opfer häufig mit Preisen, die eigentlich zu gut sind, um wahr zu sein.

Auch stark eingeschränkte Bezahlmöglichkeiten sollten grundsätzlich Misstrauen erwecken. Viele Cyberkriminelle bieten vordergründig viele Bezahlmethoden an, doch im letzten Schritt bleibt oft nur die Vorkasse als einzige Auswahlmöglichkeit. In diesem Falle halte ich es für ratsam, den Einkauf abzubrechen. Es ist unwahrscheinlich, dass der Käufer seine Ware je erhält.

Neben den genannten Auffälligkeiten weisen auch mangelnde Kontaktangaben oder frei erfundene Gütesiegel oft auf gefälschte Webseiten hin. Die Handelsregisternummer sollte im Impressum jedes Unternehmens angegeben sein. Diese kann man unter handelsregister.de prüfen und auch die Echtheit der Gütesiegel ist leicht festzustellen. Falls man ein Siegel anklickt und zum Zertifikat des Anbieters weitergeleitet wird, ist es echt.

Die meisten Internetnutzer vertrauen Bewertungen im Internet. Diese sind häufig eine gute Sache, dennoch sollte man auch da stets skeptisch bleiben. Wenn diese Bewertungen beispielsweise nur innerhalb des Shops existieren oder fast in Lobeshymnen überschlagen, kann man davon ausgehen, dass sie gefälscht sind. Auch das Fehlen der Allgemeinen Geschäftsbedingungen, beziehungsweise die schlechte Sprache in der sie geschrieben sind, sollte ein Grund sein, auf der Internetseite nicht zu bestellen.

„Es gilt, sich auch für
das Unvermeidbare zu rüsten."

Wie sollte Ihrer Meinung nach ein Unternehmen mit einer Cyberattacke umgehen? Halten Sie es für ratsam, die Öffentlichkeit zu informieren?

Die Wahrscheinlichkeit für Unternehmen, Opfer einer Cyberattacke zu werden, ist höher als je zuvor. Durch die vielfältigen und modernen Angriffsmethoden sind Hacker heute immer häufiger erfolgreich. Deshalb genügt es nicht mehr einfach nur Cyber-Security-Maßnahmen zu implementieren.

Es gilt, sich auch für das oft Unvermeidbare zu rüsten: einen tatsächlichen IT-Sicherheitsvorfall. Kommunikation spielt in diesem Zusammenhang eine entscheidende Rolle. Nur wenn Unternehmen im Ernstfall effizient kommunizieren, können sie eine Cyberattacke möglichst schnell entschärfen und ihr Ausmaß begrenzen. Nur dies ermöglicht es, den Geschäftsbetrieb so gut es geht aufrechtzuerhalten und einen Reputationsverlust zu verhindern.