

Interview zu Penetrationstests mit Christian Ehlen

## Sich der Gefahrenlage bewusst werden



Christian Ehlen, Consultant IT-Security bei Twinsec.

Bild:  
Twinsec

**Nur die Spitze des Eisbergs? Finanzinstitute mit ihren primären Geldflüssen werden von allen Seiten attackiert. Durch ihr verstärktes Engagement im Internet hat sich ihre Gefahrenlage noch verschärft. Zu alledem sind es vermehrt professionell vorgetragene Attacken, die den Banken zu schaffen machen. Dabei wird von den Entscheidern oft nur die Spitze des Gefahreneisbergs registriert.**

Doch die meisten Sicherheitsrisiken – sie liegen unterhalb der Erkennungslinie – werden von den Entscheidern nicht erkannt und demzufolge nicht in ihren Abwehrplan aufgenommen. Christian Ehlen, Consultant IT-Security bei Twinsec, rät deshalb den Finanzinstituten, sich erst einmal ihrer tatsächlichen Gefahrenlage bewusst zu werden, um geeignete Gegenmaßnahmen ergreifen zu können. Er plädiert in diesem Zusammenhang für professionell durchgeführte Penetrationstests. Das Wissen um die tatsächlichen Risiken für die Geldgeschäfte zahle sich schnell nicht nur in einem angemessenen, kostenvertretbaren Abwehrschirm aus. Auch Compliance, die nachweisliche Befolgung der gerade im Finanzbereich zahlreichen Vorschriften und Richtlinien, profitiere davon.

Sie empfehlen den Finanzinstituten, einem tragfähigen Sicherheitskonzept einen professionellen Penetrationstests vorzuschicken?

**Christian Ehlen:** Neben anderen Techniken aus der statischen und dynamischen Softwareanalyse, ist der Pen-Test ein probates Mittel um Schwachstellen aufzudecken. Vor allem Konfigurations-, Implementierungs- und Designfehler können durch dieses Mittel transparent gemacht werden. Nicht nur das: Professionell durchgeführte Pen-Tests machen deutlich, welche Schwachstellen welche potenziellen Gefahren mit welchen Auswirkungen für die Geldgeschäfte nach sich ziehen. Das bewahrt die Entscheider davor, an den richtigen Stellen zu wenig und an den falschen Stellen zu viel in IT-Sicherheitstechniken und andere Vorkehrungen zu investieren. Pen-Test sind also ein probates Mittel, die Kosten und Aufwendungen für die Sicherheit so gering wie möglich zu halten und ein angemessenes Risikomanagement zu etablieren. In welchem Bereich erachten Sie die Ausgangslage für die Finanzinstitute als besonders gefährlich?

**Christian Ehlen:** Große Gefahren holen sich Banken und Sparkassen zweifellos durch Onlinebanking ins Haus. Rund zwei Drittel aller Kunden sind mittlerweile auf diesen Zug aufgesprungen. Die Risiken des Onlinebanking sind deshalb so hoch, weil über diese Plattformen tausende von Personen und unterschiedliche Programme interagieren. Organisierte Internetverbrecher nutzen spezielle Banking Malware, um die Webapplikationen und die damit verbundenen Kundenclients zu attackieren.

Die Risiken, attackiert zu werden, sind aber nicht nur beim Onlinebanking, sondern generell im Finanzbereich hoch. Das liegt daran, dass viele der geschäftlichen Transaktionen Geldtransaktionen sind. Das weckt natürlich die Begierde von Angreifern, beispielsweise Beträge zu ihrem Nutzen zu manipulieren. Die Gefahr geht in Zeiten des Internets nicht zwangsläufig von

außen aus. Für Insider, beispielsweise auch für eigene Mitarbeiter, kann es besonders lukrativ sein, Manipulationen vorzunehmen oder mit gestohlenen Daten zu handeln.

Wir raten deshalb in diesem hochgefährlichen und veränderlichen Angriffsfeld, Pen-Tests zur Prüfung der Gefahrenlage nicht nur einmalig, sondern regelmäßig durchzuführen. So sollten die Entscheider gerade in wirtschaftlichen Stresslagen und bei einer härteren Gangart gegenüber den eigenen Mitarbeitern die Bedrohungen von innen keinesfalls unterschätzen.

Was macht Pen-Tests zu einem geeigneten Waffenset für eine wirtschaftlich ausgeprägte Sicherheit, ein angemessenes Risikomanagement und eine gezielte Gefahrenabwehr?

**Christian Ehlen:** Pen-Tests fußen auf praxiserprobten Methoden, die, sofern die Auswahl des Anbieters stimmt, genau auf den Finanzbereich und die hier drohenden Attacken abgestimmt sind. Wichtig ist, dass solche Tests ingenieurmäßig vorbereitet und durchgeführt werden. Dann liefert die anschließende Bewertung genaue Erkenntnisse darüber, welche Schutzmaßnahmen – Sicherheitswerkzeuge, Prozesse, Regeln – an welchen Stellen eingezogen werden sollten. So erreicht das Finanzinstitut so viel Sicherheit wie nötig, aber nicht mehr Sicherheit als notwendig. Wie professionelle Pen-Tests absolviert werden sollten, ist außerdem im BSI-Dokument „Durchführungskonzept für Penetrationstests“ beschrieben. Unverzichtbar für professionelle Pen-Tests ist, dass damit die unterschiedlichen Sicht- und Angriffsweisen der Angreifer antizipiert werden.

Können Sie genauer auf diese unterschiedlichen Sicht- und Angriffsweisen eingehen?

**Christian Ehlen:** Die Art und Qualität der Attacken ist vom Kenntnisstand des jeweiligen Angreifers abhängig. Je mehr er über die installierte IT und Sicherheitswerkzeuge sowie andere Sicherheitsvorkehrungen weiß, um so gezielter und verheerender wird er attackieren können. Professionelle Pen-Tests nehmen die unterschiedlichen Kenntnisstände der Angreifer auf. White-Box-Tests gehen vom weiterführenden Informationsstand eigener Mitarbeiter oder noch weiterführendem Informationsstand der Systemadministratoren aus. Black-Box-Tests nehmen die Strategien externer Hacker und Betrüger auf, die die erforderlichen internen Informationen für ihre Attacken vorher beschaffen müssen. Grey-Box-Tests greifen das ungefähre Wissen von unter anderem Geschäftspartnern, Zeitarbeitskräften und Ex-Administratoren auf und bilden es auf die Angriffsformen und potenziellen Folgen für das Institut ab.

Auch das Maß an Aggressivität kann sich in einem mehr oder weniger hohem Schaden für das Finanzinstitut auswirken. Inwieweit nehmen Pen-Tests diese psychologische Komponente auf?

**Christian Ehlen:** Wir unterscheiden deshalb bei unseren Pen-Tests in unterschiedliche Aggressivitätsstufen, außerdem in „verdeckte“ und „offensichtliche Handlungen“. Mit dieser Differenzierung kommen wir den Angriffsformen, ihren Ausprägungen und den Folgen noch näher. Dadurch rundet sich für das Finanzinstitut das potenzielle Angriffs- und Schadensbild ab, um noch gezieltere und angemessenere technische und organisatorische Vorkehrungen treffen zu können. Ein Grundproblem in vielen Finanzinstituten ist, dass für mehr kostenvertretbare Sicherheit die unterschiedlichen Fachabteilungen nicht an einem Strang ziehen. Kann diese Haltung nicht auch die Durchführung und Ergebnisse von Pen-Tests gefährden?

**Christian Ehlen:** Erfolgreiche Pen-Tests setzen eine enge Zusammenarbeit nicht nur zwischen den Testspezialisten und dem Institut, sondern auch den darin angesiedelten Fachabteilungen voraus. Das fachspezifische Wissen wird gebraucht, um die Risiken identifizieren, bemessen und, sofern wirtschaftlich vertretbar, durch Gegenmaßnahmen abstellen oder zumindest eingrenzen zu können. Dafür muss innerhalb der involvierten Fachabteilungen mittels klarer Regeln und Vorschriften diese Sicherheit auch gelebt, also befolgt werden.

Das hört sich nach einem insgesamt hohen Aufwand für Pen-Tests an – oder?

**Christian Ehlen:** Diesem Trugschluss unterliegen leider noch viele Unternehmen. Natürlich ist der Erfolg von Pen-Tests maßgeblich von der Qualität der internen Kommunikation und Koordination abhängig. Stimmt diese Basis, sind beinahe sämtliche Penetrationstests einschließlich aller Auswertungen je nach Größe des Finanzinstituts binnen fünf bis 20 Manntagen absolvierbar. Aufwendungen und Ertrag – eine nachweislich höhere Sicherheit unter geringst möglichen Kosten stehen damit für Banken, Sparkassen und Versicherungen in einem exzellenten Verhältnis. Angesichts der wachsenden Gefahr im Finanzbereich, Opfer von Attacken zu werden, also die tatsächliche Gefahrenlage zu ignorieren und einfach stillzuhalten, ist jedenfalls keine Alternative.

Zumal sich eine lückenhafte Sicherheit in eine ebenso lückenhafte Compliance auswirkt. In diesem Fall drohen Strafzahlungen und Reputationsverluste in voller Breite. Gerade Finanzinstitute sollten sich dieser Gefahr, über eine hinreichende Sicherheit nicht hinreichend compliant zu sein, keinesfalls aussetzen.

Wieso ist der Compliance-Druck auf die Finanzinstitute besonders hoch?

**Christian Ehlen:** Banken, Sparkassen und Versicherungen arbeiten nicht nur direkt mit Geld, sondern auch mit hochsensiblen (Kunden-)daten. Ihnen wird deshalb ein besonders integrierter und vertraulicher Umgang mit Geld und Daten abverlangt. Ein Umgang, den sie lückenlos bei internen Revisionen und bei externen Anfragen, inwieweit bestehende Vorschriften und Richtlinien eingehalten wurden, nachweisen müssen. Und in keinem Bereich sind die Auflagen so hoch wie im Finanzbereich. Zu nennen sind hier KonTraG, das Kreditwesengesetz, die Verordnungen und Verlautbarungen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und natürlich Basel II, bald Basel III.

Alle diese Vorschriften, bis auf Basel III, gab es aber schon vorher, ohne dass sie uns die Finanz- und Wirtschaftskrise erspart haben.

**Christian Ehlen:** Viele dieser Vorschriften und Richtlinien wurden angesichts der durchlebten und noch zu durchlebenden Krisenerfahrungen verschärft oder werden noch verschärft werden. Außerdem werden die Finanzinstitute diesmal alle Regeln gründlicher befolgen und ihre Einhaltung penibler dokumentieren müssen. Denn auch die Regierungen, Gesellschaften und Finanzdienstleistungsüberwachungen sind sensibler und kritischer geworden. Sie werden, stärker als in der jüngsten Vergangenheit, auf eine lückenlose und nachweisliche Umsetzung aller gesetzlichen Vorschriften und Richtlinien drängen.

Woher der Wind für Finanzinstitute weht, wird zudem an der Folgeversion von Basel II, Basel III, mit deutlich strengeren Regeln für eine hinreichende Eigenkapitalausstattung, eine eingehende Bewertung operativer Risiken und mehr Transparenz der Geldgeschäfte deutlich. Bereits Ende diesen Jahres soll, unter Druck der Europäischen Kommission und der

USA, die endgültige Kalibrierung von Basel III stehen.

Das Interview führte Hadi Stiel, freier Journalist in Bad Camberg.

#### Weitere Bilder

Bild 2 von 2

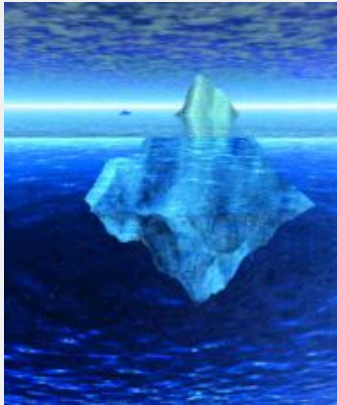


Bild: Bob Davies Fotolia.com

### Barmenia: Tests zur IT-Sicherheit

---

Barmenia Versicherungen führt regelmäßig Tests zur IT-Sicherheit durch, um ihre Sicherheitsrisiken abschätzen zu können, ihr Sicherheitsniveau zu verifizieren und ständig zu verbessern. „Dazu sind wir gesetzlich verpflichtet“, erläutert Dr. Uwe Fasting, angesiedelt innerhalb der Abteilung IT-Integration der Barmenia Versicherungen. Darüber hinaus wolle man den Kunden und Geschäftspartnern für mehr Vertrauen ein hohes Maß an nachweislicher Sicherheit bieten. Mit der Durchführung der Pen-Tests hat die Versicherung Twinsec beauftragt. „Wir verständigen uns auf die Ziele. Die verantwortlichen Techniker unseres Hauses waren und sind über die Inhalte und den Zeitrahmen der Pen-Tests immer genau informiert“, erklärt Fasting. Das Barmenia-Team kann auf die Ergebnisse stolz sein. „Die systematische Aufbereitung der Auswertungen hat uns konkrete, praktische Verbesserungspotenziale aufgezeigt“, so Fasting.