Neue SWIFT-Regeln für Finanzdienstleister

Unbezahlbar

André Clerc

Um ein Haar wäre es Hackern im vergangenen Jahr gelungen, einen der größten Betrugsfälle aller Zeiten durchzuziehen und eine knappe Milliarde US-Dollar zu erbeuten. Der SWIFT-Verbund macht nun Druck, die IT-Security in dem Bankennetzwerk flächendeckend zu stärken.

Es war eine Aktion, die das Zeug zum Krimi hatte. Im Februar 2016 schafften es bis heute unbekannte Hacker, das Zahlungsnetzwerk von SWIFT für ihre kriminellen Zwecke auszunutzen. Sie missbrauchten Zugriffsrechte und Systeme der Bangladesh Bank, um 35 Zahlungsaufträge mit einem Gesamtwert von über 950 Millionen US-Dollar vom Konto der Bank bei der Federal Reserve Bank of New York (New York FED) direkt ins SWIFT-Netzwerk einzuspeisen. Beinahe wäre den Hackern ein unglaublicher Coup gelungen, hätten nicht weiterführende manuelle Kontrollen den größten Schaden verhindert.

Nichtsdestotrotz gelang es den Hackern, fünf der 35 Zahlungsaufträge abzuwickeln. Der Schaden war damit immer noch erheblich, da rund 81 Mio. US-Dollar auf vier private Bankkonten der Hacker auf den Philippinen gelangten (weitere Informationen dazu sind über ix.de/ix1712104 zu finden). Eine Rückverfolgung dieser Zahlungen sowie des weiteren Transaktionsverlaufs war in der Folge nicht mehr möglich.

Schwierige Suche nach der Schwachstelle

Die Suche nach potenziellen Schwachstellen erwies sich als überaus schwierig. Zwar zeigte sich schnell, dass die SWIFT-seitigen Komponenten (Software, Hardware, Schutzsysteme, SWIFT-Netzwerk et cetera) nicht betroffen waren. Ausgenutzt wurden stattdessen kundenseitig unzureichend geschützte Umgebungen, Endsysteme und Accounts. Zusätzlich wurden Softwarekomponenten, beispielsweise ein PDF-Reader, so verändert, dass man manipulierte Zahlungen nicht mehr erkennen konnte. Gelingt es Hackern, an Administratorrechte eines SWIFT-Nutzers zu gelangen, kann das Bollwerk der SWIFT einen möglichen Schaden nur noch beschränken. Basierend auf den Erkenntnissen der Schwachstellensuche veröffentlichte SWIFT im Mai 2016 eine Erklärung, wonach jeder SWIFT-Nutzer – also Inhaber eines Business Identifier Code (BIC 8) – sich weiterhin um die interne Sicherheit selbst kümmern muss. Zudem sei künftig eine Selbstdeklaration zum Status der internen IT-Sicherheit einzureichen.

Die Nachrichtenagentur Reuters berichtete in der Folge, dass das Eindringen in die Systeme der geschädigten Bank vor allem einer unzureichenden Sicherheitsinfrastruktur geschuldet sei (siehe „Alle Links“). So sei ungeeignete und unzureichende Hardware eingesetzt worden, zudem habe man an wichtigen Stellen auf wirksame Schutzsysteme wie Firewall und Vulnerability Scanner verzichtet – fatale Fehler, die es Hackern letztendlich leicht gemacht hatten, das Unternehmen zu infiltrieren.

Es zeigte sich, dass das IT-Sicherheitskonzept der betroffenen Bank erhebliche Mängel aufwies. Zudem waren die Angreifer nicht nur über die eingesetzte Software und IT-Infrastruktur genauestens informiert, sondern wussten auch exakt, wo die Schwachstellen lagen und zu welchem Zeitpunkt ihr Angriff erfolgen musste.

Um herauszufinden, worin die Sicherheitslücken bestanden, die den Betrugsfall ermöglichten, trafen sich Vertreter von Bangladesh Bank, Federal Reserve Bank of New York und SWIFT. Ihr Ziel war es, nicht nur die Kriminellen aufzuspüren, sondern auch alle Details zum Fall aufzuklären, damit das globale Finanzsystem zukünftig gegen solche Attacken besser geschützt werden kann.

Die Befürchtung, dass weitere Attacken im ähnlichen Stil folgen könnten, bestätigte sich: Im Verlauf des Jahres informierte SWIFT über Angriffe mit Schadsoftware, bei denen durchweg wieder bankseitige Komponenten betroffen waren. Auch bei diesen Attacken blieben das eigene Messaging-System und die Software der SWIFT unversehrt.

Das Vorgehen der Hacker war jedes Mal dasselbe und unterschied sich kaum von anderen Angriffen. Zuerst verschafften sie sich einen Zugriff auf die kundenseitig genutzten Systeme eines Finanzinstituts. Im zweiten Schritt gelangten sie an die Benutzerdaten von Mitarbeitern, die SWIFT-Nachrichten erstellen, bestätigen oder versenden können. Danach wurden mit den gestohlenen Benutzerdaten gefälschte Nachrichten eingeschleust und mögliche Spuren sowie Beweismaterial beseitigt oder verfälscht.

Für das Verfälschen von Nachweisen manipulierten die Täter einen PDF-Reader, den die betroffenen Mitarbeiter des

Finanzinstituts für das Lesen der SWIFT-Nachrichten nutzten. Dieser war bereits vorher als Schadsoftware auf den Arbeitsrechnern installiert worden und unterschied sich äußerlich kaum vom Original. Wurde der Reader jedoch zum Lesen der Zahlungsbestätigungen verwendet, wurden die entsprechenden Dokumente verfälscht dargestellt oder sogar ganz gelöscht.

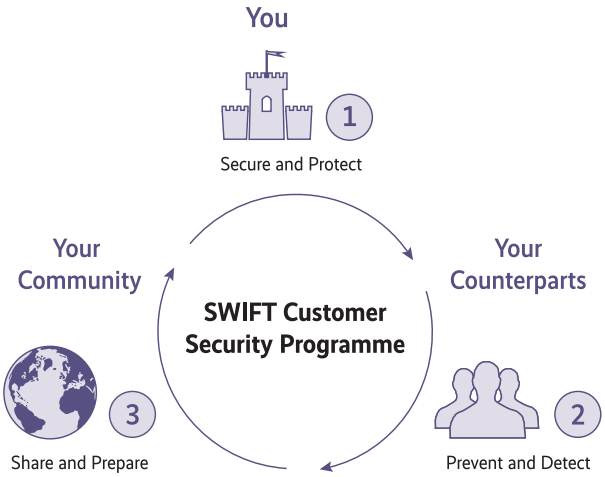
In allen bekannten Betrugsfällen nutzten die Cyberkriminellen ausschließlich Schwachstellen der kundenseitig eingesetzten IT-Systeme aus, um manipulierte SWIFT-Nachrichten über das SWIFT-Netzwerk zu versenden. Die entsprechenden Kontrollen und Schutzmechanismen der Finanzinstitute wurden umgangen. Was aber noch viel schwerer wog: Durch das Löschen oder Verfälschen der Auszüge und Bestätigungen waren die Opfer erst mit Verzögerung in der Lage, den Betrug zu erkennen.

Ein so perfide geplanter Angriff hätte theoretisch jeden treffen können, da es sich bei den Angreifern um hochprofessionelle kriminelle Organisationen handelt. Diese loten alle erdenklichen Schwachstellen aus und setzen dort an, wo sie den schlechtesten Schutz vorfinden.

IT-Systeme auf dem Prüfstand

Um das Einschleusen gefälschter Zahlungsaufträge in Zukunft zu verhindern, sah der SWIFT-Verband keinen anderen Weg, als bestimmte Vorgaben zur Verwendung seiner Infrastruktur an alle SWIFT-Nutzer (Finanzinstitute, Pensionskassen, Industriekonzerne et cetera) zur Bedingung zu machen. Die Sicherheit der kundenseitigen Umgebungen und insbesondere der Kanäle für Datenübertragungen sowie den Zahlungsverkehr sollte dabei im Mittelpunkt stehen. Denn eines stand fest: Die Täter mussten sich vor ihrem großen Coup über längere Zeit sehr tief in die IT-Systeme der betroffenen Organisationen gehackt haben.

Mit den Vorgaben zur Nutzung der SWIFT-Infrastruktur sind alle Teilnehmer aufgefordert, detailliert darüber zu informieren, wie sie sich gegen Cyberangriffe schützen. Umgekehrt ersuchten die Nutzer selbst SWIFT um Hilfestellung auf diesem Gebiet. Die Vorgaben alleine sind aber nach Ansicht von SWIFT noch nicht ausreichend, einem möglichen Schaden vorzubeugen. Deshalb sind die Nutzer auch ausdrücklich zum zeitnahen Informationsaustausch bei Verdacht auf einen Betrugsfall aufgefordert.



Das SWIFT CSP bezieht für Sicherheit und Schutz nun auch die Aspekte Vorbeugen und Erkennen sowie den Informationsaustausch und das Vorbereiten bei möglichen Betrugsfällen ein. Früher wurde kundenseitig lediglich der Schutz der eigenen Umgebung gefordert (Abb. 1).

Unter den Stichworten „Secure and Protect“, „Prevent and Detect“ sowie „Share and Prepare“ hat der SWIFT-Verbund seine Customer-Security-Programme (SWIFT CSP) ins Leben gerufen. Ein erster Entwurf wurde Ende Oktober 2016 allen Nutzern zur Prüfung zugestellt. Er war vor allem auf kleinere SWIFT-Nutzer mit rudimentärer IT-Sicherheitsinfrastruktur ausgelegt.

Stolpersteine für große Organisationen

Großen Organisationen erschienen die im Entwurf enthaltenen Maßnahmen als zu wenig praktikabel und es kam daher von ihrer Seite starker Widerstand: Ihre bereits vorhandenen, professionellen Sicherheitssysteme wären durch diese neuen Maßnahmen quasi ausgehebelt worden und kontrollierte automatisierte Prozesse hätten zumindest teilweise durch manuelle Abläufe ersetzt werden müssen.

Es folgte eine Stellungnahme des SWIFT-Verbunds, in der auch die Schweizer Teilnehmer mit Bezug auf diese negativen Folgen zu Wort kamen. Daraufhin wurden die Vorgaben überarbeitet. Zwar blieben die detaillierten Empfehlungen weiterhin gültig, sie wurden jedoch durch großzügigere Freiräume für alternative Umsetzungen ergänzt.

Die nun geltenden Sicherheitsvorgaben, die im SWIFT Customer Security Controls Framework festgehalten sind, verlangen den kundenseitigen Schutz der Komponenten, die direkt an das SWIFT-Netzwerk angeschlossen sind. Pflicht wird auch das wirksame Schützen und Einschränken der Anmeldeinformationen (Credentials), die dem Zugriff auf SWIFT-Systeme dienen, sowie das Reagieren auf mögliche Angriffe.

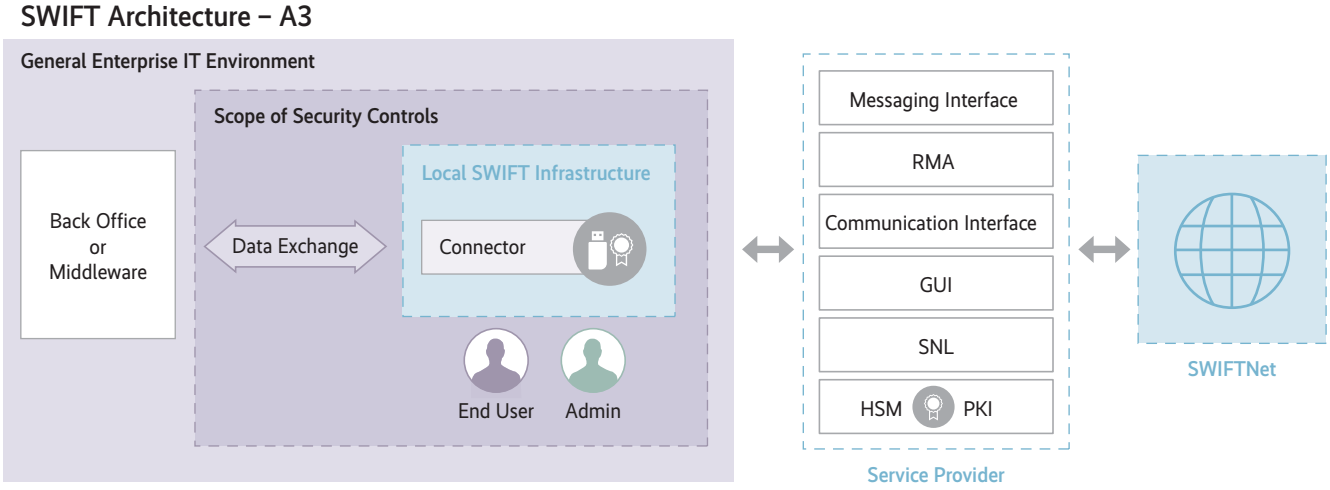
Die SWIFT-Vorgaben entsprechen im Grundsatz den Maßnahmen, die in größeren Organisationen mit hohem Sicherheitsbewusstsein bereits umgesetzt oder zumindest zur Umsetzung geplant sind. Es ist trotzdem davon auszugehen, dass ein großer Teil der SWIFT-Nutzer notwendige Verbesserungen am Sicherheitskonzept umsetzen muss.

Mit dem geforderten Geltungsbereich geht SWIFT deutlich weiter als beispielsweise die Finanzmarktaufsicht in Deutschland, Österreich und der Schweiz. Die Vorgaben richten sich nicht nur an Banken und Finanzinstitute, sondern an alle Inhaber einer achtstelligen BIC. Dies bedeutet, dass die Vorgaben künftig weltweit auch für Versicherer, Pensionskassen und Industriekonzerne gelten. Selbst wenn ein BIC-Inhaber die SWIFT-Dienstleistungen über ein Servicebüro bezieht, bleibt er umsetzungspflichtig und muss eine Selbstdeklaration über die je nach Infrastrukturtyp 16 oder 11 zwingenden Sicherheitskontrollen („Security Controls“) einreichen (Abbildung 2).

Da es sich bei SWIFT nicht um einen Regulator handelt, beziehen sich die neuen Vorgaben nur auf SWIFT-Komponenten. Es ist jedoch dringend zu empfehlen, die geforderten Maßnahmen konzernweit umzusetzen und alle IT-Komponenten miteinzubeziehen. Auf diese Weise kann die Sicherheit eines Unternehmens als Ganzes erhöht werden. Ein zentrales Element ist eine starke Authentifizierung der Mitarbeiter gegenüber den IT-Systemen, was letztlich zu einem wirksamen Schutz vor dem Diebstahl von Credentials führt.

Mit einer firmenweiten Umsetzung der für die SWIFT-Komponenten geforderten Sicherheitsmaßnahmen hätten auch viele der spektakulären und medienwirksamen Hackerangriffe aus den letzten Monaten verhindert oder zumindest in ihrer Wirkung begrenzt werden können. Dazu gehören die WannaCry- und NotPetya-Attacken, die weltweit verheerende Schäden in Unternehmen, Krankenhäusern und Behörden anrichteten.

In weiteren Fällen, beispielsweise dem Heartbleed-Programmfehler, der neben prominenten Websites auch VoIP-Telefone, Router und Netzwerkdrucker für Angriffe anfällig machte, wäre mit einem



Die vorgegebenen Maßnahmen hängen unter anderem vom Typ der Infrastruktur ab. Neben weiteren drei Architekturtypen wird bei diesem Typ eine Softwareanwendung (im Beispiel Alliance Lite2 AutoClient zum Dateienaustausch) innerhalb der Kundenumgebung verwendet, um die Kommunikation zwischen Anwendungen mit einer Schnittstelle zu einem Dienstleister auszustatten (Abb.2).

effizienten Incident- und Change-Management ein schnelleres Patchen der betroffenen Systeme möglich gewesen.

Angelehnt an andere Standards

Mit den aktuell definierten Maßnahmen und Kontrollen hat die SWIFT das Rad nicht neu erfunden. Vielmehr lehnen sich die Sicherheitskontrollen eng an internationale Standards wie das Cybersecurity Framework des National Institute of Standards and Technology (NIST), ISO/IEC 27002 oder den Sicherheitsstandard der Kreditkartenwirtschaft PCI DSS (Payment Card Industry Data Security Standard) an (siehe „Alle Links“). Sie lassen sich sogar auf diese Standards übertragen (sogenanntes Mapping), um bestehende Sicherheitsinfrastrukturen auf SWIFT-Komponenten anzuwenden.

Obwohl die SWIFT-Nutzer nur 11 beziehungsweise 16 der insgesamt 27 Schutzziele zwingend erfüllen müssen – die anderen sind nur „empfohlen“ –, ist als effektiver Schutz vor Angriffen auch hier eine vollständige Umsetzung der Maßnahmen ratsam.

Unter anderem sollten dabei folgende Punkte in den Mittelpunkt rücken:

- Schutz der lokalen (SWIFT-)Umgebung;
- Kontrolle privilegierter Konten auf dem Betriebssystem;
- Sicherheit der internen Datenströme;
- Sicherheitsupdates regelmäßig einspielen;
- Systemhärtung: Analyse der Systeme und anschließende Härtung, um die Verwundbarkeiten zu reduzieren;
- starke (Multi-Faktor-)Authentifizierung und logische Zugriffskontrolle (Access Control);
- Schutz gegen Malware optimieren;
- Softwareintegrität überprüfen;
- Logging und Monitoring von Aktivitäten;
- Planung der Abwehrmechanismen bei Cyberattacken.

Insbesondere den letzten Punkt sollte man nicht vernachlässigen: Wer keinen Plan zur Abwehr von Angriffen ausgearbeitet hat, geht ein hohes Risiko ein – es drohen finanzielle Einbußen sowie Imageschäden. Die meisten größeren Organisationen besitzen zwar einen solchen Plan, bei vielen mittleren und kleinen Unternehmen hapert es damit aber noch. Kein Wunder, dass sich sogar die amerikanische Homeland Security mit dem Thema beschäftigt und amerikanische Unternehmen zum Handeln auffordert („Alle Links“).

SWIFT macht Druck

Für die SWIFT-Nutzer wird die Zeit langsam knapp, denn bereits bis Ende Dezember 2017 müssen alle Inhaber einer sogenannten BIC 8 eine Selbstdeklaration einreichen, die den Erfüllungsgrad der vorgeschriebenen Sicherheitskontrollen angibt. Das einmalige Einreichen reicht jedoch nicht aus: Die Selbstdeklaration muss mindestens alle zwölf Monate erneuert werden, Gleiches gilt bei einer Änderung der lokalen IT-Systemumgebung.

Im Januar 2018 führt SWIFT zudem ein Monitoringsystem ein und erhöht den Kooperationsdruck auf die Teilnehmer. Ab dann kann den Regulatoren – etwa der Eidgenössischen Finanzmarktaufsicht (FINMA) für die Schweiz, in Deutschland der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und in Österreich der Finanzmarktaufsicht (FMA) – übermittelt werden, welche Organisationen die Selbstdeklaration bis dato nicht eingereicht haben. Bis Dezember 2018 schließlich muss die volle Regelkonformität (Compliance) zu den SWIFT-Vorgaben erreicht sein. Auch hier sieht die SWIFT vor, die Konformität zu überwachen und den Regulatoren diejenigen Institute zu melden, die die Regeln nicht erfüllen.

Für diejenigen, die bei der Analyse und Umsetzung der SWIFT-Vorgaben externe Unterstützung benötigen, hat SWIFT eigens ein Verzeichnis von registrierten Cybersecurity-Providern erstellt („Alle Links“).

Mit der Umsetzung der SWIFT-Vorgaben und den Empfehlungen seitens NIST, BSI oder ISO/IEC wird es für Cyberkriminelle wesentlich schwerer, ihre Ziele zu erreichen. Dazu wird es aber notwendig sein, die aktuellen Maßnahmen und Vorgaben regelmäßig auf den Prüfstand zu stellen – insbesondere mit Blick auf die hochprofessionellen, bestens organisierten und stark motivierten Angreifer, die unermüdlich auf der Suche nach neuen Zielen sind. Und trotz aller Bemühungen wird es kriminellen Organisationen auch in Zukunft immer wieder gelingen, das schwächste Glied einer Kette auszumachen und auszunutzen. (ur)

André Clerc

ist Expert IT-Security Consultant der TEMET AG sowie Referent für PKI und seit über 17 Jahren in der IT-Security tätig.

Alle Links: www.ix.de/ix1712104