Gion Sialm vom BIT und Ivan Bütler von Compass Security teilen mit AdNovum CTO Tom Sprenger ihre Erfahrungen mit Web-Security.

Sicher ins Web statt ins Netz

Die Sicherheitssituation im Web verändert sich laufend. Gion Sialm vom BIT, Marc Condrau von Health Info Net und Ivan Bütler von Compass Security diskutieren am Security-Round-Table mit unserem CTO Tom Sprenger über aktuelle Entwicklungen.

Attacken sind bekanntlich der grosse Gegenspieler der Security. Welche Angriffe richten heute den grössten Schaden an?

IB: Die Hauptgefährdung geht von Attacken über Trojaner aus. Firmen mit grossen Forschungsabteilungen, deren langfristiger Erfolg von eingereichten Patenten abhängt, kämpfen mit dem permanenten Versuch von Hackern, an ihr geistiges Eigentum zu gelangen. Auch Spionageaktivitäten von Staat zu Staat werden primär über den Einsatz von Trojaner-Software realisiert.

Die zweite Gefahr sind Insidergeschichten. Traditionelle Phishing-Attacken sind im Web-Kontext rückläufig, da sie oft mühsam und aufwändig sind. Heute hacken sich Angreifer ins Content Management System (CMS) börsenkotierter Firmen, um beispielsweise den Quartalsabschluss ein paar Stunden vor Publikation zu bekommen. Besitzt das Hacker-Team das notwendige Know-how, um den Quartalsabschluss zu interpretieren, können an der Börse hochspekulative Geschäfte getätigt werden.

MC: Phishing-Attacken und Trojaner waren und sind auch aus Sicht von HIN die relevantesten Gefahren. Zentral ist aus unserer Sicht der Schutz des Endpunkts, typischerweise des Benutzer-PCs. Wichtig ist hier die Benutzerfreundlichkeit. Denn Benutzer werden Sicherheitslösungen mit ungenügender Usability umgehen. Ein weiterer zentraler Punkt ist, das Bewusstsein der Benutzer zu schärfen.

Was erwartet ein Benutzer heute von einem Online-Portal betreffend Sicherheit?

(Die Teilnahme von Marc Condrau erfolgte schriftlich.)

IB: Mir persönlich sind der Schutz und die Integrität meiner Daten wichtig. Bei der Nutzung kostenloser Angebote wie Facebook, Twitter und Co. weiss ich, dass ich die Kontrolle aus der Hand gebe und mit meinen Daten bezahle. Von einer Business-Applikation erwarte ich jedoch, dass sie meine Daten nicht weitergibt, die Vertraulichkeit gewährleistet und die geltenden regulatorischen Bestimmungen einhält. So müssen etwa beim Online-Bezahlen mit Kreditkarte die Standards der PCI (Payment Card Industry) berücksichtigt werden. Deshalb darf zum Beispiel die Kreditkarten-CVC (dreistelliger Code) von den Anbietern nicht gespeichert werden.

MC: Im Gesundheitswesen kommt dem Datenschutz enorme Bedeutung zu. Beim Datenzugriff und Datenaustausch sind höchste Vertraulichkeit und die sichere Identifikation der Kommunikationsteilnehmer zwingend. Andererseits sollen die relevanten Gesundheitsdaten den Behandelnden jederzeit umfassend zur Verfügung stehen. Dieser Balanceakt stellt bei der Gestaltung von Security-Systemen für das Gesundheitswesen eine Herausforderung dar.

Daten werden zunehmend organisations- und systemübergreifend genutzt. Wie sichern Sie innerhalb des Unternehmens den Zugriff ab?

GS: Beim Bund gibt es klare Bestimmungen, nicht nur beim Access Management, sondern auch beim Datenschutz. Es darf nicht möglich sein, aufgrund von Zugangsdaten Rückschlüsse auf eine Person zu ziehen. Hat zum Beispiel jemand Zugriff auf die Mehrwertsteuer, ist es wahrscheinlich, dass er ein eigenes Unternehmen besitzt. Das lässt wiederum weitere Rückschlüsse zu. Deshalb braucht es eine saubere Datentrennung. Jedes Amt sieht nur das, was es selber verwaltet. Dabei stellen wir die Datentrennung nicht nur über Vorgaben und Prozesse sicher, sondern auch technisch. Das macht die Lösungen zwar komplexer, ist aber wichtig für den Datenschutz.

IB: Als Grundregel empfehle ich, die Zugriffskontrolle möglichst nahe bei den Daten vorzunehmen. Zentral ist auch die professionelle und sichere Programmierung der Webapplikation. In der Praxis können jedoch Fehler in der Implementation nicht zu 100% ausgeschlossen werden. Es ist deshalb eine weise Strategie, Webapplikationen zusätzlich durch eine vorgeschaltete Web Application Firewall (WAF) zu schützen, damit ein solcher Fehler nicht gleich zum Super-GAU führt. Dies gilt insbesondere dann, wenn man keinen Zugriff auf den Source Code der Webapplikation hat.

MC: Weitere Grundvoraussetzungen für den sicheren externen Zugriff auf interne Daten und Funktionen sind die zuverlässige Authentisierung und Autorisierung der Benutzer. Hier setzt HIN als Identity und Access Service Provider für das Gesundheitswesen an: Der Einsatz validierter HIN-Identitäten entlastet Applikationsanbieter im überinstitutionellen Datenaustausch. Die HIN-Entry-Server-Infrastruktur stellt die Perimeter-Security für die angeschlossenen Applikationen sicher, beispielsweise für Radiologiesysteme von Spitälern, und übernimmt die applikatorische Autorisierung der externen Benutzer.

> Es ist eine weise Strategie, Webapplikationen zusätzlich durch eine vorgeschaltete Web Application Firewall zu schützen. (Ivan Bütler)

Schaut man sich die Entwicklungen bei den Webapplikations-Architekturen an, stellt man einen Trend in Richtung «App in a Browser» fest. Es werden nicht mehr bei jedem Call GUIs hin- und hergeschickt, sondern die ganze Applikation läuft im Browser (zum Beispiel HTML5). Die Kommunikation mit dem Backend wandelt sich dabei zur technischen Datenkommunikation. Wie verändert das die Anforderungen an eine WAF-Lösung?

IB: Die technischen Calls folgen Standards wie RESTful Services, JSON oder XML. Die WAF muss diese Protokolle und Technologien verstehen und validieren können. Probleme gibt es bei «getunnelten» Protokollen und Protokollen ohne offene Standards (wie ICA oder früher GWT), weil die WAF diese nicht validieren kann. Solange das Web proprietäre Formate zur Übermittlung von Daten zulässt, kann eine WAF auf dieser Ebene keinen umfassenden Schutz bieten.

Sind die neuen HTML5-Applikationen auch ein Thema beim Bund?

GS: Ja, wir nutzen HTML5-Applikationen in Kombination mit WAF und Reverse Proxy. Dadurch gewinnen wir Flexibilität und können an verschiedenen Orten bezüglich Sicherheit eingreifen. Weil Sicherheit für uns zentral ist, müssen wir bei den unterstützten Security Features immer auf dem aktuellsten Stand sein. Wir entwickeln unsere Security-Architektur laufend weiter und schauen, was wir wiederverwenden können und was neu unterstützt werden muss.

Zurück zum Thema Datensicherheit: Zunehmend trifft man auf Anwendungsfälle, in denen Daten den Bereich von geschützten Systemen verlassen, da sie etwa einem Dritten zur Verfügung gestellt werden. Beispiele dafür sind Cloud-Dienste oder in der Zusammenarbeit mit Partnern genutzte kollaborative Services. Die klassische Perimeter-Security greift hier nicht mehr. Trotzdem wollen wir die Kontrolle über die Daten behalten. Was gibt es hier für Ansätze?

IB: Nehmen wir als Beispiel ein E-Banking, das auch «fremde» Daten in Form von Kreditkartenabrechnungen darstellt. Die Ownership der Kreditkartenabrechnungen liegt nicht bei der Bank, sondern beim Kreditkartenunternehmen. Das E-Banking bezieht einen Feed vom Kreditkartenhersteller und generiert damit Mehrwert für den E-Banking-Kunden. Hier sehe ich zwei Security-Aspekte. Erstens: Die Daten des Anbieters (Kreditkartendaten) können schadhafte Elemente enthalten. Die Bank sollte deshalb diese Daten validieren, auch wenn sie von einem vertrauenswürdigen Partner stammen, da sonst das Risiko einer sogenannten Second-Order Injection besteht. Zweitens gibt das Kreditkartenunternehmen die Ownership über die Kreditkartendaten preis. Was die Bank damit macht, hängt von der vertraglichen Regelung ab. Der Kunde weiss nicht mehr, wo seine Daten liegen.

Gibt es Instrumente, um mit dem Zielkonflikt zwischen Data Privacy und Data Exchange umzugehen? Zum Beispiel im Kontext von Government- oder E-Health-Lösungen würde die Aggregation von Nutzdaten sicher Mehrwert bringen. Doch müssten die Bürger dazu akzeptieren, dass ihre Daten den Einflussbereich der Organisation verlassen.

GS: Eine Aggregation könnte durchaus Mehrwert bieten. Dies ist einfach geregelt, indem solche Datenbestände eine gesetzliche Grundlage brauchen. Wenn also Daten im Amt oder amtsübergreifend aggregiert werden, beruht dies zwangsläufig auf einer hierzu bestehenden Gesetzesgrundlage. Dies gewährt, dass Daten nicht ohne Zustimmung der Politik analysiert oder aggregiert werden.

MC: Im Gesundheitswesen ist die Aggregation der besonders schützenswerten Gesundheitsdaten mit anderen Daten ein heikler Punkt. Die E-Health-Strategie des Bundes trägt diesem Umstand Rechnung, indem für das elektronische Patientendossier nicht die AHV13-Nummer als Patientenidentifikator verwendet wird, sondern ein eigener Patientenidentifikator.

Bedeutet das für Unternehmen und Organisationen, dass sie ihre Identitäten und Authentisierungsmittel in einem zeitaufwändigen und teuren Vorhaben konsolidieren müssen?

GS: Nicht unbedingt. Wir haben eine föderative Architektur aufgebaut und es innerhalb von weniger als einem Jahr geschafft, in der Bundesverwaltung mit PKI, Kerberos, Name/Passwort, Name/Passwort/SMS und SuisseID zu authentisieren.

> Mit HTML5-Applikationen und einer Second Line of Defense erreichen wir eine hohe Sicherheit und Flexibilität.
> (Gion Sialm)

Ist es nach Ihrer Einschätzung in der Regel sinnvoll, einen Identitäts-Pool zu haben und zentral zu verwalten?

MC: Ja, davon sind wir überzeugt. HIN bietet für das Gesundheitswesen Identitäten in der Cloud als Service an. Tauschen Institutionen untereinander Daten aus, braucht der Applikationsanbieter die Identitäten nicht aufwändig zu identifizieren und zu registrieren. Die Benutzer erhalten mittels Single Sign-on Zugriff auf über 50 Anwendungen. Um Föderierung zu ermöglichen, haben wir das HIN Access Gateway entwickelt.

IB: Föderierte Dienste haben auch nach meiner Einschätzung ein hohes Zukunftspotenzial. Die Unternehmen werden dazu übergehen, die Identitäten ihrer User über Dienste wie Active Directory Federation Services (ADFS) im Internet nutzbar zu machen, so dass Cloud-Anbieter von diesen Identitäten profitieren können. Das spart Zeit und Geld.

Ein interessanter Ansatz. Die Unternehmen verwalten die Identitäten und schliessen mit Cloud-Anbietern einen Vertrag ab. Wird eine neue Identität erfasst, wird sie automatisch in Richtung Cloud-Anbieter provisioniert.

IB: Und umgekehrt: Verlässt ein Mitarbeiter die Firma, wird sein Account auf dem unternehmenseigenen Active Directory und im Federation Service gesperrt. Die Sperrung ist unmittelbar und sofort wirksam. Der Benutzer kann nach der Sperrung weder das Firmennetz noch die aktivierten föderierten Services nutzen. Leider sind föderierte Systeme komplex. Die Verbreitung und Nutzung braucht entsprechend noch etwas Reifezeit.

MC: Die Provisionierung kann auch von der Cloud in das interne IAM erfolgen. Gerade im Gesundheitswesen mit der hohen Mobilität der Mitarbeitenden ist dieser Ansatz interessant: Validierte Identitätsdaten, einschliesslich Informationen zu den medizinisch-fachlichen Qualifikationen, können beim Eintritt in eine Organisation übernommen werden.

Föderierte Dienste haben ein hohes Zukunftspotenzial. (Ivan Bütler)

Es gibt hier den schönen Begriff «Dynaxität» – wir erhöhen zugleich die Dynamik, indem wir die Identitäten föderiert brauchen, und die Komplexität, indem wir mehr Services ansteuern. Das verlangt nach einer strengeren Governance …

GS: Definitiv. Früher war die Governance schneller als die Technik. Vor allem die monolithischen Architekturen waren so komplex, dass wir jahrelang daran bauten. Heute hinkt die Governance der Technik hinterher. Und die Kunden sind «hungrig», haben Erwartungen. Wir brauchen ein gutes Gespür dafür, was wir zulassen wollen, ohne dass die Komplexität überhandnimmt.

Schlagen wir den Bogen zur Authentisierung. Das ist besonders im Mobile-Bereich ein aktuelles Thema, denn die Erwartungen an die Benutzerfreundlichkeit sind hier generell hoch. Welche Trends beobachten Sie da?

MC: Bei mobilen Geräten verwenden die Benutzer von HIN-Services aktuell primär mTAN und weniger die kartenbasierten Verfahren. Derzeit prüfen wir MobileID.

IB: Die Authentisierung muss vor allem einfach sein. Komplizierte zertifikatsbasierte Lösungen wie SuisseID werden sich meiner Meinung nach in der Breite nicht durchsetzen. Die Chance für solche Systeme sehe ich in geschlossenen Umgebungen (zum Beispiel Bund) oder bei Anwendungen mit erhöhten Sicherheitsbedürfnissen (B2B oder Ähnliches).

GS: Für E-Government sind nur zwei Dinge notwendig: eine flexible IAM-Architektur und ein gutes, einfaches Authentisierungsmittel. Wir haben zwar PKI, doch ist das Gerät so gross wie das Mobile selbst. An der SuisseID schätzen wir, dass wir den Verwaltungsaufwand auslagern können.

Wie könnte eine einfache Authentisierung aussehen?

IB: Die Benutzername/Passwort-Authentisierung ist so erfolgreich, weil sie einfach ist. Es braucht keine Software, man muss nichts kaufen oder installieren und jeder beherrscht sie. Allerdings erachte ich diese Art der Authentisierung als nicht besonders sicher. Die Sicherheit kann erhöht werden, indem das Verhalten und die Eigenschaften des Client Computers bei der Authentisierung analysiert werden. Ein sogenannter «Client Correlator» überprüft die Settings des Client Computers des Anwenders, beispielsweise Bildschirmauflösung, installierte Plugins, Sprache des Browsers, durchschnittliche Loginzeit bei der Authentisierung und IP Range des Providers. Solche Informationen verraten schon fast, wer an einem Computer sitzt, bevor sich der User mit Passwort einloggt. Die EFF (Electronic Frontier Foundation) hat unter dem Projekt «Panopticlick» einen Prototyp erstellt, der diese Technik vorführt.

MC: Im Gesundheitswesen ist eine einfache Benutzername/Passwort-Authentisierung bei einem externen Zugriff inakzeptabel. Um das Verfahren für die Applikationsanbieter zu vereinfachen, bietet die HIN-Plattform vier verschiedene Authentisierungsverfahren an: zertifikatsbasiert mit Soft Token, mTAN, Health Professional Card der FMH und SuisseID.

Spinnen wir den Gedanken weiter: Wären Lösungen denkbar, bei denen man sich nicht explizit einloggen muss, solange man nichts Riskantes tut?

IB: Ein adaptives Sicherheitssystem – das ist eine gute Idee und wäre für den Benutzer sehr bequem. Doch bei Fällen wie etwa

einer Mehrwertsteuer-Rückzahlung bräuchte es einen Step-up auf ein höheres Security-Niveau. Und dieser müsste vom Aufwand her vertretbar sein. Muss der Benutzer am Ende trotzdem ein Client-Zertifikat zur Authentisierung installieren, könnte er das gleich von Anfang an tun.

Werden die Attribute von einem Client Correlator gesammelt, besteht eine gewisse Unschärfe in der Einschätzung. Ist dieses Risiko aus Ihrer Sicht vertretbar?

MC: Für den Zugriff auf Personendaten im Gesundheitswesen ist ein Zugriff ohne explizite Authentisierung nicht denkbar.

GS: Beim Bund bräuchte es definitiv ein Umdenken. Für gewisse Fälle wie der vorher erwähnten Mehrwertsteuer-Rückzahlung kann eine solche Technik aber nur in Kombination mit einem Verfahren eingesetzt werden, das jegliche Unschärfe ausschliesst.

IB: Letztlich läuft es darauf hinaus, über die Analyse der Daten aus dem Client Computer eine Vorhersage über den Benutzer zu machen. Systeme, die solche Techniken einsetzen, wissen im Prinzip schon vor der Authentisierung, wer am anderen Ende der Leitung arbeitet. Der Einsatz solcher Profiling-Systeme ist in der Kreditkartenindustrie bereits Standard. Mit jeder Kreditkartentransaktion bezahlt man ein paar Rappen in einen Schadenpool. Die Kreditkartenunternehmen wissen genau Bescheid, wann und wo eine Kreditkarte genutzt wird. Findet in Südamerika eine Belastung statt, während der Inhaber selbst in Europa sitzt, wird dies automatisch erkannt und der Inhaber bleibt schadlos. Das Kreditkartensystem lebt mit dem latenten Risiko eines Missbrauchs. Dieses Paradigma kann man auch auf andere Businessfälle anwenden.

> Profiling wäre denkbar, um Zugriffe bei ungewöhnlichem Nutzerverhalten zu unterbinden. (Marc Condrau)

Könnte die nächste Generation von Security allenfalls ein Profiling einbeziehen?

GS: Wie bereits erwähnt, bedarf ein Profiling einer gesetzlichen Grundlage. Obwohl auch Schweizer Bürger zunehmend ihre persönlichen Daten für Profiling an Unternehmen oder soziale Netzwerke abgeben, ist es noch schwer denkbar, dass dies im Verwaltungsumfeld zugelassen würde.

MC: Im Gesundheitswesen wäre ein Profiling in dem Sinne denkbar, dass Zugriffe unterbunden werden, wenn das Benutzerverhalten ungewöhnlich ist. Also zum Beispiel dann, wenn ein Zugriff auf Gesundheitsdaten aus dem Ausland erfolgt. Die Sinnhaftigkeit hängt aber stark vom Anwendungsfall ab.

IB: Im Profiling, also in der Erstellung und Verwendung von Profilen von Benutzern wie auch von Anwendungen, Netzwerkverkehr und Ähnlichem, sehe ich grosses Zukunftspotenzial. Die Korrelation von Daten wird für Forschung und Sicherheit zentral sein.

Wie wir sehen, sind die Möglichkeiten der Datennutzung im Web noch lange nicht ausgeschöpft. Gleichzeitig werden die Benutzer immer anspruchsvoller und die Angreifer immer professioneller. Der Schutz unserer Daten bleibt damit auf absehbare Zeit ein aktuelles Thema. Ich danke Ihnen für das spannende Gespräch. ■

Round-Table-Teilnehmer:

Gion Sialm

Gion Sialm ist als Leiter IAM im BIT zuständig für den Zugang zu Bundesapplikationen. Dieser zentrale Service im Bund fungiert fast ausschliesslich als Trust Broker. Auf flexible Art und Weise werden intern wie extern gehostete Applikationen mit den grössten Authentisierungsverzeichnissen inner- und ausserhalb des Bundes verbunden, wobei die Bewirtschaftung der Zugriffe jeweils in der Kontrolle und Verantwortung der beauftragenden Ämter bleibt.

Marc Condrau

Marc Condrau ist Lösungsarchitekt und Projektleiter bei der Health Info Net AG (HIN). HIN wurde 1996 auf Initiative des Dachverbandes der Schweizer Ärztinnen und Ärzte (FMH) und der Ärztekasse gegründet mit dem Ziel, den Schweizer Gesundheitsfachpersonen die sichere Nutzung des Internets zu ermöglichen. Kerndienst von HIN ist das Identity Providing für Leistungserbringer (aktuell zirka 17000). Auf Basis der HIN-Identitäten werden Secure-E-Mail-Dienste und Access Control Services angeboten. Nahezu alle niedergelassenen Leistungserbringer und über 420 Institutionen nutzen HIN Mail und über 50 Applikationsanbieter nutzen die Access Control Services.

Ivan Bütler

Ivan Bütler ist Co-Gründer und CEO der Compass Security. Das 1999 gegründete Unternehmen mit Büros in Jona, Bern und Berlin beschäftigt 35 Personen und ist spezialisiert auf Ethical Hacking, Penetration Testing und Security Reviews. Ivan Bütler ist Lehrbeauftragter an den Fachhochschulen Rapperswil und Luzern und organisiert für Swiss Cyber Storm die European Cyber Security Challenge. Er ist der geistige Vater des Hacking-Lab, eines internationalen Labors für Security Professionals.