Bildquelle: Fotolia

SPECIAL: HACKING DAY 2012 – FUTURE SECURITY

IN KOOPERATION MIT DIGICOMP

Incident Response – irgendwann trifft's jeden

IT-Sicherheitsvorfälle werden von den betroffenen Unternehmen oft totgeschwiegen – ein nicht immer richtiger Ansatz, wie der Fall DigiNotar zeigt. Christoph Baumgartner

Der gute Ruf und Daten, wie beispielsweise das Kundenverzeichnis, Konstruktionspläne, Forschungsaufzeichnungen, Rezepturen oder Source Codes, sind entscheidende Assets moderner Unternehmen, die oft mit viel Fleiss, Zeit und Geld erschaffen wurden. Umso ärgerlicher ist es, wenn diese Werte quasi zum Nulltarif von Dritten empfindlich beschädigt oder gar entwendet werden. Besonders hart hat es DigiNotar getroffen, einen holländischen Anbieter von digitalen Zertifikaten, der aufgrund einer erfolgreichen Hackerattacke im September 2011 Konkurs anmelden musste. Doch was war geschehen?

DigiNotar stellte digitale Zertifikate aus, die als elektronische Identitätskarten im Internet dienen. Mit ihnen lassen sich beispielsweise Banken und Betreiber von Onlineshops die Echtheit ihrer E-Banking-Portale und Onlineshops bestätigen, indem sie sich von Zertifizierungsstellen (Certification Authority, CA) wie eben DigiNotar auf ihre Identität hin überprüfen lassen. Nach erfolgreicher Überprüfung stellt die CA ein SSL-Zertifikat aus, das die Bank oder der Betreiber des Onlineshops auf dem Webserver

Christoph Baumgartner ist CEO und Inhaber der auf Security Consulting und anspruchsvolle Security Audits spezialisierten OneConsult GmbH. Am Hacking Day am 14. Juni 2012 bei Digicomp spricht Christoph Baumgartner über das Thema «Incident Response» in der Keynote am Nachmittag.

> **Seite 49**
Hacking Day 2012 – Future Security

> **Seite 50**
Programm

installiert. Die Besucher des Webservers können ab diesem Zeitpunkt die Identität des Anbieters verifizieren, indem das Zertifikat vom Browser beim Herausgeber des entsprechenden Zertifikats auf seine Gültigkeit hin verifiziert wird. Die Sicherheit steht und fällt somit mit der Vertrauenswürdigkeit der Gültigkeitsbestätigung und der CA.

Was lief schief?

Einem oder mehreren Hackern war es gelungen, trotz Sicherheitsmassnahmen digital in die Systeme von DigiNotar einzudringen und über mehrere Tage hinweg mehr als 500 gefälschte Zertifikate auszustellen. Der Fall wäre wohl nicht so rasch publik geworden, wenn nicht prominente Organisationen und Dienste wie Facebook, Google, Microsoft, Skype, Twitter und die CIA betroffen gewesen wären. Das Problem bei gefälschten digitalen Zertifikaten im Vergleich zu gefälschten Papieren ist, dass Fälschungen genauso echt wie das Original aussehen und nur indirekt aufgrund der Verknüpfung mit einem «falschen» Server erkennbar sind.

Dieser Vorfall traf die anerkannten Zertifizierungsstellen im Internet, deren Modell auf Vertrauen basiert, empfindlich. So mussten die Softwarehersteller so rasch wie möglich neue Softwareversionen oder Patches veröffentlichen, die die von DigiNotar herausgegebenen Zertifikate als ungültig erkennen.

DigiNotar wusste gemäss den Untersuchungsergebnissen bereits seit mehreren Tagen von der laufenden Hackerattacke, schien aber mit dem Vorfall überfordert zu sein. So beschloss man, die Attacke zu verheimlichen und nach deren Bekanntwerden herunterzuspielen. Diese fatale Strategie führte DigiNotar direkt in den Konkurs, weil das Haupt-Asset, die Vertrauenswürdigkeit, quasi über Nacht wegfiel. Dieses schädliche Verhalten hat Einfluss auf die Reputation aller CAs.

Korrektes Vorgehen und Default Best Practices

Eines vorweg: Es gibt bei Hacker- und Malware-Attacken oder Datenklau nicht das eine richtige Vorgehen, sondern es geht darum, die Strategie mit den geringsten (potenziell) unerwünschten Nebenwirkungen zu erkennen und konsequent umzusetzen. Folgende Empfehlungen sollen als Hilfe dienen, haben aber keinen Anspruch auf Vollständigkeit:

Alarmieren: Bei Sicherheitsvorfällen muss als Erstes der IT-Sicherheitsverantwortliche beziehungsweise die für derartige Vorfälle zuständige Stelle (CISO, IT-Leiterin, Rechtsdienst etc.), aber zumindest der Vorgesetzte informiert werden, mit Angaben über Zeitpunkt, Art des Vorfalls, Auswirkungen und Ausmass des bisher erkennbaren Schadens.

Reflektieren: Jetzt gilt es, einige Fragen zu klären – eine kleine Auswahl: Wie hoch ist der zu erwartende Schaden in zeitlicher Abhängigkeit? Soll nur direkte Schadensbegrenzung betrieben werden oder möchte man sich die Option offenhalten, rechtliche Schritte gegen den Verursacher einzuleiten? Wie hoch ist das Risiko, unbeteiligte / nicht massgeblich beteiligte Dritte zu belangen? Welche Lösungsansätze mit welchen technischen, organisatorischen, rechtlichen, finanziellen, das Firmen-Image betreffenden direkten und indirekten Konsequenzen kommen in Betracht?
Da einige juristische Stolpersteine existieren, sollte die Rechtsabteilung nach Möglichkeit in die Entscheidungsfindung einbezogen werden. Bei computerforensischen Unterfangen müssen zwingend entsprechende Spezialisten beigezogen werden, da hinsichtlich Beweissicherung, Analyse und Dokumentation strikte Regeln eingehalten werden müssen. Nur so ist die Verwertbarkeit vor Gericht gewährleistet.

Reagieren: Sobald ein Entscheid gefallen ist, gilt es klar zu kommunizieren und entsprechende Massnahmen zu ergreifen und zu dokumentieren.

Hacker- und Malware-Attacken: Falls das System auf Kosten einer möglichen Strafverfolgung möglichst rasch wieder verfügbar sein soll, gilt folgendes Standardvorgehen:

1. Das betroffene System temporär vom Netz nehmen;
2. die letzte nicht kompromittierte Datensicherung einspielen;
3. das System anschliessend härten;
4. das System mittels eines Security-Scans oder Penetration-Tests auf Sicherheitslücken überprüfen und falls nötig erneut härten;
5. erst dann wieder ans Netz anschliessen.

Datenklau: Bei In-flagranti-Situationen den Sicherheitsdienst oder die IT-Sicherheitsverantwortlichen rufen lassen, die betroffene(n) Person(en) nach Möglichkeit an weiteren Manipulationen und am Verlassen des Raumes hindern, ohne handgreiflich zu werden! Vermeintliche Heldentaten sind hier fehl am Platz.

Vorbeugen ist besser als nachbessern

Technische Massnahmen wie Firewalls, Virenscanner, Netzwerk-Zonierung und Datenverschlüsselung sollten heute selbstverständlich sein. Aber genauso wichtig sind organisatorische Massnahmen wie eine Risikoanalyse und -beurteilung (welchen Gefahren ist das Unternehmen ausgesetzt, wie hoch sind Eintrittswahrscheinlichkeit und potenzielle Schadenshöhe?), die Klassifikation von Informationen/Daten (was ist überhaupt schützenswert?), das Verfassen von zielgruppengerechten Handlungsanweisungen (Policies), die Definition einer IT-Sicherheitsorganisation (IT-Sicherheitsverantwortlicher rapportiert an wen und hat welche Pflichten und Kompetenzen?), Change-Management-Prozesse (was wird wann, wie und von wem gemacht?) und detaillierte Notfallpläne, damit feststeht, wie in welchem Szenario zu agieren ist.

Die Szenarien müssen in sogenannten Notfallübungen durchexerziert werden. Andernfalls herrscht im Ernstfall garantiert Chaos. Eine Hilfestellung zu möglichen Massnahmen findet sich beispielsweise in der ISO/IEC-Normenfamilie 2700x oder in den BSI-Standards 100-x.

Fazit

IT-Sicherheitsvorfälle durch Dritteinwirkung können einer Organisation ernsthaften Schaden zufügen. Doch es existieren Mittel und Wege, wie Unternehmen sich schützen und negative Folgen verhindern oder vermindern können.

Hacking Day 2012 – Future Security

Datenschutz in der Wolke, Bring your own Device (BYOD), mobile Geräte mit sensiblen Daten, immer mehr Webapplikationen und rechtliche Aspekte wie Revision und Schutz der Privatsphäre machen aus einem IT-Security-Verantwortlichen einen Experten, der in vielen Bereichen detailliert Bescheid wissen muss. Die elf Referate, Workshops und Praxisberichte mit Live-Demos des Hacking Day 2012 decken diese Breite ab. Die Keynote von Thomas Dübendorfer, Senior Software Engineer bei Google, startet mit Cloud-Diensten und BYOD-Herausforderungen.

An diesem Hacking Day erhalten Sie viele Tipps, um Angriffe abzuwehren. Aber seien wir ehrlich: Niemand ist zu 100 Prozent vor einem Cyber-Einbruch geschützt. Christoph Baumgartner, CEO der OneConsult GmbH, bringt in der Keynote am Nachmittag Beispiele, was Sie nach einem Einbruch in Bezug auf Recht, Technik und Organisation unbedingt tun sollten.

Stellen Sie sich aus den Referaten und Workshops Ihr Wunschprogramm zusammen. Die Platzzahl ist beschränkt – sichern Sie sich Ihren Platz!
www.digicomp.ch/hackingday

HACKING DAY 2012

- Datum: 14. Juni 2012
- Ort: Digicomp Zürich, Limmatstrasse 50, 8005 Zürich
- Kosten: 350.–, inkl. Kaffee, Gipfeli, Lunch und Apéro
- Details und Anmeldung: www.digicomp.ch/hackingday
- Alle Teilnehmenden erhalten nach der Veranstaltung die Vorträge zum Download zur Verfügung gestellt.

Die Referenten:

Dr. Thomas Dübendorfer
Dr. Dübendorfer arbeitet als Senior Software Engineer bei Google in Zürich im Bereich Security und weiss aus eigener Erfahrung, was es bedeutet, global verfügbare Webapplikationen in der Praxis gegen Bedrohungen abzusichern. Für seine Beiträge zur Absicherung von Googles weltweitem Online-Werbesystem AdWords/AdSense hat er Googles «EMG award for impact and innovation» erhalten. Zudem amtet er als Präsident der swisssecurity.org und ist Dozent an der ETH Zürich. Er hat einen Doktortitel und einen Dipl. Informatik-Ing. ETH Masterabschluss mit Auszeichnung der ETH Zürich und hat zudem das Höhere Lehramt absolviert.
www.google.ch

Umberto Annino
Umberto Annino ist als Manager im Bereich IT-Audit/Risk Assurance bei PwC tätig. Nach seinem Einstieg in die Informatik mit einer Lehre als KV-Anwendungsentwickler hat er sich kontinuierlich weitergebildet, den Abschluss NDS FH Qualitätsmanagement gemacht und sich auf das Thema Informationssicherheit fokussiert. Neben der Tätigkeit als IT-Auditor ist Umberto bei ISACA Switzerland Chapter sowie der ISSS Information Security Society Switzerland im Vorstand aktiv und unterrichtet das Thema Informationssicherheit, IT-Risikomanagement und Datenschutz an verschiedenen Schulen. Umberto ist zertifiziert als CISA, CISM, CRISC, CGEIT sowie CISSP, CISSP-ISSMP und CISSP-ISSAP.
www.pwc.ch

Reto C. Zbinden,
Rechtsanwalt, CEO, Swiss Infosec AG
Reto C. Zbinden, Gründer und Inhaber der Swiss Infosec AG, beschäftigt sich seit fast 25 Jahren als unabhängiger Berater und Trainer mit Informationssicherheit. Seine Spezialgebiete sind strategische Fragen der Integralen Sicherheit / Informationssicherheit / Risk Management, Sicherheitsorganisation, Zertifizierungen im Bereich der Informationssicherheit und die rechtlichen Aspekte der Informationssicherheit, so unter anderem Archivierung, Datenschutz und Vertragsrecht im Bereich Informations- und IT-Sicherheit. In seinen Mandaten legt er den Fokus stets auf Praxiskonformität, Wirtschaftlichkeit und Good Practice.
www.infosec.ch

Ivan Bütler
Ivan Bütler is the co-founder and CEO of Compass Security AG, a Swiss Ethical Hacking and Penetration Testing company located in Rapperswil Switzerland with a brand in Nürnberg Germany. Several of his publications on network and computer security have raised international recognition. Besides his own business he is also a tutor at both the University of Applied Sciences in Rapperswil and Lucerne University of Applied Sciences and Arts. Ivan is a regular speaker at international conferences. He is in the board of the Swiss Cyber Storm 3 Conference Committee, CTO of Hacking-Lab and co-founder of the Cyber Tycoons anti-warfare foundation. Additionally, he is in the board of the ISSS Swiss Security Society Foundation since 2010. **www.csnc.ch/de**

Andreas Wisler, Dipl. IT Ing. FH,
CISSP, ISO 27001 Lead Auditor, MCITP Enterprise Server Administrator
Andreas Wisler ist Geschäftsführer der GO OUT Production GmbH, die sich mit ganzheitlichen und produktneutralen IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. Penetration Tests und Social Engineering runden das Profil ab. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (INFONEWS) heruntergeladen werden kann.
www.goout.ch

Christoph Baumgartner
Christoph Baumgartner ist CEO und Inhaber der OneConsult GmbH, einem international tätigen, Schweizer IT-Security-Consulting-Unternehmen mit Hauptsitz in Thalwil und Büro in Wien. Er studierte an der Universität Zürich Wirtschaftsinformatik (MSc UZH IS) und ist seit 1996 als Berater mit den Schwerpunkten IT-Security und IT-Strategie tätig. Bevor Baumgartner 2003 mit dem Aufbau der OneConsult GmbH begann, war er in diversen Führungsfunktionen bei verschiedenen namhaften System- und Security-Integratoren tätig. Seine Spezialgebiete sind konzeptionelle Security Audits, Sicherheitsrichtlinien und -konzepte, BCM- und Disaster-Recovery-Coaching sowie strategische Beratung. Baumgartner ist OSSTMM Professional Security Tester und ISECOM Board Member. **www.oneconsult.com/de**

Martin Rutishauser
Martin Rutishauser ist Mitglied von Defcon-Switzerland und arbeitet für die Datalynx AG in Basel als Information Security Consultant / Penetration Tester, ist zudem für die Hochschule Luzern (CAS/MAS IS) als Referent tätig. 10 Jahre Erfahrung im IT- und Informationssicherheitsbereich garantieren einen spannenden Vortrag.
www.datalynx.ch/site

Tobias Ellenberger
Tobias Ellenberger ist COO und Teilhaber der seit 2003 auf anspruchsvolle Security Audits nach OSSTMM spezialisierten, international tätigen, hersteller- sowie produktunabhängigen OneConsult GmbH. Bis 2007 arbeitete er als IT-Consultant und System Engineer in verschiedenen Firmen. Er wirkte als Projektleiter und Consultant in einem internationalen Unternehmen und war zuständig für das Engineering und die Weiterentwicklung von neuen und bestehenden IT-Infrastrukturlösungen mit Fokus auf Security, Unified Messaging und Virtualisierung. Seit April 2010 ist Tobias Ellenberger bei OneConsult im technischen Security Consulting und seit September 2011 Mitglied des Managements. Er ist OSSTMM Professional Security Tester und OSSTMM Professional Security Analyst. **www.oneconsult.com/de**

Programm des Hacking Day 2012 – Future Security

08:30 – 09:00	Eintreffen / Registrierung		
09:00 – 10:00	 **Dr. Thomas Dübendorfer:** Neue Sicherheitsherausforderungen durch «Cloud Computing» und «Bring Your Own Device»		
10:00 – 10:15	Pause		
10:15 – 11:00	 **Martin Rutishauser:** Portscanning im Jahre 2012	 **Reto C. Zbinden:** Mitarbeiterkontrolle versus Datenschutz: legal oder illegal? Egal? Nein!	 **Andreas Wisler:** Penetration Test – Möglichkeiten und Nutzen
11:00 – 11:15	Pause		
11:15 – 12:00	 **Ivan Bütler:** OWASP (Open Web Security Application Project) TOP 10	 **Umberto Annino:** IT-Revision, IT-Risiken und die Hacker – wie weit schauen die Revisoren?	
12:00 – 13:00	Lunch		
13:00 – 13:45	 **Christoph Baumgartner:** Incident Response – so reagieren Sie richtig		
13:45 – 14:00	Pause		
14:00 – 14:45	 **Ivan Bütler:** OWASP TOP 10 – Hack & Learn	 **Tobias Ellenberger:** Android Smartphones und Sicherheit	 **Dr. Thomas Dübendorfer:** Sichere Entwicklung von Webapplikationen anhand eines Online-Ticketshops
14:45 – 15:00		Pause	
15:00 – 15:45		 **Tobias Ellenberger:** OWASP Mobile Top 10	
15:45	Apéro		

Inhalte der einzelnen Vorträge und Anmeldung unter: www.digicomp.ch/hackingday