Prevention, Detection and Response: Wieso reine Prävention nicht (mehr) reicht

Adrian Bachmann

Viren, Würmer, Trojaner, Phishing, Drive-by Attacken und Social Engineering [1] sind nur eine kleine Auswahl der möglichen Angriffsmittel, welche von kriminellen Kreisen eingesetzt werden, um gewinnbringende Angriffe auf Informationssysteme vorzunehmen. Die Professionalisierung der kriminellen Seite hat dabei erschreckende Ausmasse angenommen. Längst sind es nicht mehr (nur) gelangweilte Computernerds in dunkeln Kellern, welche Systeme hacken, sondern vielmehr ist es ein florierender (Schwarz-)Markt mit ausgeklügelten Standardwerkzeugen für den Bau von massgeschneiderter Schadsoftware [2] bis hin zur Denial of Service Attacke as a Service. Kundensupport, Service Level Agreements sowie Erfolgsgarantien und erfolgsabhängige Vergütungsmodelle sind dabei längst Realität. Kann der Webshop des Konkurrenten nicht genügend lange vom Netz genommen werden, so wird der Auftrag wiederholt – kostenlos. Trojaner attackieren mit einer vom Verkäufer garantierten Erfolgsrate Computersysteme, verschlüsseln sämtliche Daten und fordern vom Benutzer ein Lösegeld, um wieder an die Daten zu kommen. Wird nicht bezahlt, wird das Schlüsselmaterial unwiderruflich vernichtet und ein Zugriff auf die Daten ist nicht mehr möglich. Teilweise schlummern solche Trojaner über Wochen unbemerkt auf den Systemen, so dass auch das letzte Datenbackup ebenfalls nur verschlüsselte Daten enthält. Zahlen und auf die Ehrlichkeit des Angreifers hoffen oder aber den Datenverlust hinnehmen sind dabei vielfach die einzigen Optionen, die einem Opfer bleiben.

Dabei sind diese Businessmodelle nicht ganz neu. Blicken wir in die physische Welt, so entdecken wir diverse Parallelen sowie jahrhundertlange Erfahrung. Gleiches gilt, wenn es darum geht, sich vor solchen Angriffen zu schützen. In der physischen wie auch der virtuellen Welt wird dabei gerne von den Disziplinen Prevention, Detection und Response gesprochen. Am Beispiel eines Juweliers lassen sich diese gut veranschaulichen: Gehärtetes Schaufensterglas sowie eine ausgeklügelte Schliessanlage sollen Einbrüche verhindern (Prevention). Sollte dennoch eine Diebesbande eindringen können, so wird dies dank Sensoren und einer Alarmanlage erkannt (Detection) und sofort die Polizei alarmiert, welche ausrückt und versucht, die Diebesbande noch vor der Flucht zu fassen (Response). Zurück in der virtuellen Welt möchte ich dazu einladen, kurz darüber nachzudenken, welche Massnahmen Sie zum Schutz vor Angriffen umgesetzt haben. Spontan werden Sie möglicherweise an Virenscanner, Firewalls, starke Passwörter, aktuell gehaltene Software und eventuell gar an Verschlüsselung denken. Dabei handelt es sich jedoch fast ausschliesslich um Massnahmen der Prävention – sprich Massnahmen die einen Angriff verhindern sollten. Gerade in Zeiten von Zero-Day Exploits und massgeschneiderten sowie ausgeklügelten Phishing Attacken reicht jedoch die reine Prävention definitiv nicht mehr, denn es besteht die Möglichkeit, dass jemand ohne unser Wissen einen Generalschlüssel zu unserem Juweliergeschäft gefunden hat und diesen jederzeit einsetzen kann.

Dr. Adrian Bachmann *studierte Wirtschaftsinformatik an der Universität Zürich und verfasste dort auch seine Dissertation zum Thema Datenqualität im Software Engineering Prozess. Nach einigen Jahren im IT Projekt- und Risikomanagement bei einer grösseren Schweizer Bank berät er seit 2011 seine Kunden in Themen der Informationssicherheit und leitet entsprechende Projekte.*

Kontaktadresse:
Dr. Adrian Bachmann
Partner, IT Security Consultant
TEMET AG
Basteiplatz 5
CH-8001 Zürich
Tel: +41 79 464 01 46
E-Mail: adrian.bachmann@temet.ch
http://www.temet.ch

In der physischen Welt haben wir uns längst daran gewöhnt, dass es keine unüberwindbaren Verhinderungsmassnahmen gibt und vielfach erst die Kombination mit Detektion und Reaktion zum gewünschten Schutzniveau führt. Interessanterweise ist diese Erkenntnis in der virtuellen Welt jedoch noch nicht überall angekommen und wir konzentrieren uns nach wie vor hauptsächlich um präventive Massnahmen. Wikipedia listet in seinem Artikel „Informationssicherheit“ [3] derzeit 14 operative Sicherheitsmassnahmen. Nur gerade zwei dieser Massnahmen weisen im Gesamtkontext einen detektiven Charakter auf. Die restlichen Massnahmen gelten der reinen Prävention. Zugegebenermassen sind Massnahmen der Detektion und Reaktion bezüglich Komplexität meist auf einem anderen Niveau als dies Massnahmen der reinen Prävention sind. Zudem erfordert die Identifikation von geeigneten Massnahmen der Detektion und Reaktion eine intensivere Auseinandersetzung mit der Risikoexposition. Dennoch sollen wir uns zur Erreichung eines angemessenen Schutzniveaus auch mit diesen Themen auseinandersetzen und die Frage stellen, wie erfolgreiche Angriffe erkannt und auf solche reagiert werden kann. Im Fokus sollte dabei ein geeignetes Zusammenspiel von Massnahmen stehen, mit welchem nicht nur klassische Angriffe auf die Infrastruktur von aussen, sondern auch Angriffe von innen oder über Mitarbeitende erfolgreich bewältigt werden können. Sie werden rasch feststellen, dass dabei nicht nur technische Massnahmen gefragt sind.

In Fachkreisen gehen die Diskussionen und Fragestellungen derweilen etwas weiter: Wie soll damit umgegangen werden, dass ein Angriff möglicherweise gar nicht erkannt und somit gar keine Reaktion eingeleitet wird? Oder wie kann nach einer verpassten oder fehlgeschlagenen Response möglichst schnell ein Recovery – spricht das wieder Erreichen des Normalzustands – durchgeführt werden?
Es ist an der Zeit, uns mit geeigneten und angemessenen Massnahmen zum Schutz von Angriffen auf die Informationssicherheit auseinander zu setzen.

[1] Siehe Glossary der Swiss Internet Security Alliance, https://www.swiss-isa.ch/de/glossar
[2] Siehe z.B. „Einbruch mit Komfort“, c’t Ausgabe 18/2015
[3] Siehe https://de.wikipedia.org/wiki/Informationssicherheit