Link: https://www.cio.de/a/threat-exchange-gemeinsam-gegen-die-organisierte-cyberkriminalitaet,2952409

Interview mit Andreas Wuchner

Threat Exchange – gemeinsam gegen die organisierte Cyberkriminalität

Datum: 04.04.2014
Autor(en): Oliver Häußler

Um sich gegen das organisierte Verbrechen wehren zu können, muss sich die Industrie besser organisieren, fordert nicht zuletzt der Gesetzgeber. Andreas Wuchner war CISO im Bankengeschäft und ist heute im Bereich Security Strategy bei HP Enterprise Security Services. Er kennt die Bedrohungen auf der Kundenseite und weiß, wie wichtig es ist, dass sich die CIOs von Banken auf Plattformen gegenseitig unterstützen.

Andreas Wuchner, Security Strategy, HP Enterprise Security Services.
Foto: HP

Die Cyberkriminellen sind bestens organisiert. Mit Plattformen wie der FS-ISAC oder ThreatCentral versuchen Organisationen und Hersteller, auch bei Anbietern und Anwendern den Community-Gedanken zu verbreiten, um sich gemeinsam gegen die Angriffe besser zur Wehr zu setzen. Wie kommt das bei CIOs an?

Andreas Wuchner: Dass sich die Banken über Sicherheitsthemen untereinander austauschen ist nicht neu. Dafür gibt es viele Beispiele aus allen Ländern, wie den Frankfurter Kreis, um nur eines zu nennen. Meist sind das sehr persönliche Beziehungen, der Informationsaustausch ist jedoch nicht mit bestehenden Systemen verlinkt und eine Reaktion auf einen Angriff tritt erst mit einem gewissen Zeitverzug in Kraft.
Auch das US-amerikanische Industrieforum für Sicherheit FS-ISAC ist eine hervorragende Community für IT-Sicherheit im Finanzbereich. Sie bietet eine Plattform auf Basis einer Mitgliedschaft für Banken, auf der wichtige Informationen ausgetauscht werden und verschickt Alerts per Mail an diese. Das Mitglied ist dann zwar informiert, dass ein Angriff stattgefunden hat, aber zur Ergreifung von Schutzmaßnahmen muss der CIO weitere Aktionen starten.

Wie schätzen Sie Akzeptanz der Banken für Threat-Exchange-Plattformen ein?

Andreas Wuchner: Die Banken wissen, dass sie in den nächsten Jahren gesetzlich zur Kollaboration verpflichtet werden, um sich zu schützen und einen gesamtwirtschaftlichen Schaden abzuwehren. Daher sind CIOs offen gegenüber Threat-Exchange-Plattformen.

Das Zusammenspiel in einer Community, wie sie auf Plattformen forciert wird, basiert auf Vertrauen. Warum sollte ein CIO einer Bank sensible Informationen über Angriffe auf sein System einem Mitbewerber mitteilen und Gefahr laufen, dass Kunden durch die Veröffentlichung das Vertrauen in die Bank verlieren?

Andreas Wuchner: Diese Sorge besteht nicht, denn es geht darum, Attacken und Bedrohungen auszutauschen, nicht Kundeninformationen. Die Daten kommen von einem Trusted Partner. Der Community-Gedanke besteht darin, dass man Informationen eingibt und selbst welche in Echtzeit beziehen kann. Daraus ergibt sich ein Informationsvorsprung gegenüber den Angreifern.

Welche konkreten Informationen müssen ins System eingespeist werden, damit es funktioniert und die Banken dennoch geschützt sind?

Andreas Wuchner: Es geht beispielsweise um Angaben über die Art der Attacke, wo sie herkommt, an wen sie sich richtet, was sie bewirkt, wer mitbetroffen sein könnte, ob sie geteilt oder zielgerichtet ist. Interessant ist auch, welches Ziel sie verfolgt, will der Angreifer Daten stehlen oder anderen Schaden anrichten? Wenn die betroffene Organisation beziehungsweise das Security Operation Center weiß, dass es Schutzmaßnahmen gibt, stellt der Verantwortliche diese Information ins System und verweist gegebenenfalls auf einen bereits bestehenden Workaround. Er beantwortet also die Frage, ob es sich um einen Zero-Day-Angriff handelt oder um eine Variante eines bekannten Trojaners, der eine bestimmte Schwachstelle ausnutzt. Mit dieser Art von Informationen können CIOs anderer Banken unmittelbar Gegenmaßnahmen oder ein gezieltes Monitoring in Gang setzen, um ihr System vor dem Angriff zu schützen.

Kennen Sie ein Beispiel für eine erfolgreiche Threat-Exchange-Abwehr?

Andreas Wuchner: Im Bereich Malware es gibt viele offene Schnittstellen, über die Organisationen den Security-Unternehmen mitteilen, sobald ein Angriff stattfindet. Dabei handelt es sich aber vorwiegend um Open-Source-Kleinprojekte. Was wir hier machen, ist der erste kommerzielle Ansatz, bei dem eine Plattform mit offenen Schnittstellen angeboten wird, über die man Informationen im großen Umfang eingeben wie auch beziehen kann. Da wir gerade erst damit beginnen, gibt es bislang noch keine Fallauswertungen dazu.

Bei welchen Arten der Kriminalität kommt Threat Exchange infrage?

Andreas Wuchner: Generell ist Security Threat Exchange bei verteilten Angriffen, bei Botnetzen und Viren am wirkungsvollsten. Generell gilt: Je ungerichteter der Angriff ist, desto erfolgreicher funktioniert das Abwehrsystem.

"Die Ursache zu bekämpfen ist ein anderer Ansatz"

Folglich funktioniert es bei zielgerichteten Angriffen nicht?

Andreas Wuchner: Im Bereich der Industriespionage wird meist sehr gezielt und individuell über persönliche Beziehungen und andere Methoden angegriffen. Hier hilft eine Informationsplattform nur bedingt weiter. Aber selbst bei Targeted Attacks ist es denkbar, dass andere von einem Austausch der Informationen profitieren können. Vielleicht gibt es ja Parallelen bei der Vorgehensweise der Angreifer, die auf andere Unternehmen übertragbar sind.

Threat Exchange erhöht die Reaktionsgeschwindigkeit und bietet Informationen zur Prävention. Die Ursache der Cyberkriminalität wird damit aber nicht bekämpft – die Verursacher werden weder verfolgt noch unschädlich gemacht. Warum?

Andreas Wuchner: Die Ursache zu bekämpfen ist ein anderer Ansatz. Wir machen Zero-Day-Initiativen und versuchen, den Markt sozusagen auszutrocknen, indem wir Belohnungen aussetzen und damit die Schädlinge aus dem Markt nehmen. Will man aber an die Verursacher selbst heran, ist das sehr schwierig, da das deutsche Recht in Drittländern, wo die Verursacher ansässig sind, in der Regel nicht anwendbar ist.

Sollte die Industrie das Thema selbst nicht in den Griff bekommen, wird der Gesetzgeber Vorgaben machen, wie er es beispielsweise bei der Meldepflicht beim Datenschutz bereits getan hat. Im geplanten IT-Sicherheitsgesetz werden weitere Auflagen diskutiert. Welche Auswirkungen werden diese auf die Unternehmen haben?

Andreas Wuchner: Die Regulatoren sehen sich immer mehr in der Pflicht, Vorgaben zu machen. Die EU-Regulation will bezwecken, dass Unternehmen und Organisationen Maßnahmen zur eigenen Absicherung und zum Schutz vor Schäden gegenüber dem Gemeinwohl ergreifen. Entsprechende Regelungen sind in absehbarer Zeit zu erwarten. Das bedeutet für Banken und andere Unternehmen, dass damit ein Mehraufwand bei der Verwaltung und bei der Ergreifung von Sicherheitsmaßnahmen hinzukommt, der aber letztendlich in deren Sinne ist, da er zu mehr Sicherheit führt.

Welches sind die wichtigsten Vorteile einer Threat-Exchange-Plattform?

Andreas Wuchner: Geschwindigkeit und Vollständigkeit. Der CIO kann sich auf die Informationen verlassen. Sie stehen ihm schnell und unmittelbar zur Verfügung. Sie bieten ihm einen Wissensvorsprung vor den Angreifern.

Oliver Häußler, freier Journalist in München
