Auf dem Weg zum Intrusion Detection System der nächsten Generation

Stefan Schumacher *

12. Januar 2010
Kaishakunin.com
IT-Sicherheitsberatung

2005 habe ich im Vortrag »Einbruchserkennung in Netzwerke mit Intrusion Detection Systemen« die Funktionsweise von IDS beschrieben. In den letzten Jahren hat sich der Hype um Snort &. Co. etwas gelegt und die systembedingten Grenzen wurden aufgezeigt. So sind IDS immer noch nicht in der Lage, unbekannte Angriffe zu erkennen oder gar das soziale System einer Organisation zu analysieren.

Ich zeige anhand von Beiträgen aus der Philosophie, Pädagogik und Psychologie, wie Erkenntnis und Lernen funktioniert und welche Voraussetzungen erfüllt sein müssen, um lernende und erkennende IDS aufzubauen.

Ein Intrusion Detection System (IDS) ist ein System, das Einbrüche bzw. Einbruchsversuche in ein Netzwerk erkennen soll.

Da ein Einbruch aber nicht nur aus TCP/IP-Paketen besteht, sondern oftmals auch auf einer sozialen Ebene wie z. B. Social Engineering, (vgl. Kehrer 2008; N.N. 2009; Schumacher 2009*a*,*b*,*c*,*d*) stattfindet, ist es notwendig diese Ebene ebenfalls zu analysieren.

Darüberhinaus sind die gegenwärtigen IDS nicht in der Lage neuartige Angriffe zu erkennen. Sie verwenden im Prinzip Lexika, in denen bereits erkannte und analysierte Angriffe aufbereitet wurden und vergleichen diese mit dem Netzwerkverkehr.

Wünschenswert sind aber IDS, die neuartige Angriffe selbständig erkennen können und aus Einbruchsversuchen lernen.

Daher versuche ich anhand der Erkenntnis- und Wissenschaftstheorie darzulegen, welche Voraussetzungen notwendig sind, um *neuartige* Einbruchsversuche zu erkennen. Außerdem stelle ich Erkenntnisse aus der psychologischen Diagnostik/Prognostik vor, die sich ebenfalls mit der Vorhersage von Sicherheitsvorfällen befasst.

Anschließend werde ich im Hauptteil Modelle aus der Pädagogischen Psychologie zeigen, die Lern- und Erkenntnisprozesse im Menschen modellieren. Mein Hauptaugenmerk liegt dabei auf der genetischen Epistemologie (Erkenntnistheorie) Jean Piagets. Diese Theorie zeigt, wie Menschen Wissen als Struktur aufbauen und so neue Handlungskompetenzen erwerben. Sie wird auch in der KI-Forschung und Kybernetik eingesetzt, um lernende Automaten zu entwerfen.

*Stefan.Schumacher@Kaishakunin.com
http://www.Kaishakunin.com

Abschließend zeige ich, ob und wie die Erkenntnisse aus der Psychologie in der IDS-Entwicklung eingesetzt werden können und welche Grenzen die Software noch hat bzw. welche Grenzen nicht überwunden werden können.

Der Vortrag stellt dabei kein fertiges Produkt, sondern Forschungsansätze vor. Grundkenntnisse über Netzwerke und IDS wären wünschenswert. Kenntnisse in Psychologie oder Philosophie nicht erforderlich.

Die Grobgliederung sieht folgendermaßen aus:

- Wozu dienen IDS? Wie ist der gegenwärtige Stand der Dinge?
- Wie funktionieren Diagnosen und Prognosen? Wie werden Entscheidungen gefällt?
- Wie funktioniert Erkenntnis und Lernen?
- Wie soll das IDS der Zukunft aussehen?
- Welchen Beitrag können IDS zur Sicherheit einer Organisation leisten?

Literaturverzeichnis

Kehrer, Anika (2008). „IT-Security psychologisch implementieren“. In: *Linux-Magazin*. Bericht vom Frühjahrsfachgespräch 2008 über den Vortrag *Design und Implementierung einer Security-Awareness-Kampagne*. URL: http://www.linux-magazin.de/NEWS/GUUG-Fachgespraech-IT-Security-psychologisch-implementieren (besucht am 22. 10. 2009). Siehe Seite 1.

N.N. (2009). „Risiken durch Manipulation per Social-Engineering“. In: *Entwickler Magazin* (2009. März 2009). Bericht vom Frühjahrsfachgespräch 2009 über den Vortrag *Psychologische Grundlagen des Social-Engineering*. URL: http://entwickler.de/zonen/portale/psecom,id,99,news,47855,p,0.html (besucht am 2009. 03. 20). Siehe Seite 1.

Schumacher, Stefan (2009*a*). „Admins Albtraum. Die psychologischen Grundlagen des Social Engineering, Teil I“. In: *Informationsdienst IT-Grundschutz* 7 (Juli 2009), Seiten 11 – 13. ISSN: 1862-4375. URL: http://grundschutz.info/fileadmin/kundenbereich/Dokumente/Grundschutz_7-2009_11_13.pdf (besucht am 22. 07. 2009). Siehe Seite 1.

– (2009*b*). „Admins Albtraum. Die psychologischen Grundlagen des Social Engineering, Teil II“. In: *Informationsdienst IT-Grundschutz* 8 (August 2009), Seiten 8 – 9. ISSN: 1862-4375. URL: http://grundschutz.info/fileadmin/kundenbereich/Dokumente/Grundschutz_8-2009_8_9.pdf (besucht am 24. 08. 2009). Siehe Seite 1.

– (2009*c*). „Admins Albtraum. Die psychologischen Grundlagen des Social Engineering, Teil III“. In: *Informationsdienst IT-Grundschutz* 10/11 (Oktober 2009), Seiten 21 – 22. ISSN: 1862-4375. Siehe Seite 1.

– (2009*d*). „Psychologische Grundlagen des Social-Engineering“. In: *Proceedings des GUUG Frühjahrsfachgespräches 2009*. Band 2009. 10. – 13. März 2009, Hochschule Karlsruhe. Köln: GUUG, Seiten 77–98. ISBN: 978-3-86541-322-2. Siehe Seite 1.