Monitoring von Cyber Attacken – Verfahren zur Anomalieerkennung

Was bedeutet Monitoring von Cyber Attacken?

Monitoring bezeichnet ein „intensives Beobachten […] der gefährdeten Ressourcen“[1] eines Systems, um eine erfolgreich durchgeführte Cyber **Attacke erkennen** zu können. Zu den Aufgaben des Monitoring zählen somit das Sammeln von Informationen, die Analyse des Datenverkehrs und die Problemdiagnose.[2]

Unter Cyber Attacken werden **nicht autorisierte Zugriffe** bzw Zugriffsversuche auf ein System verstanden.[3] Da diese Angriffe zunehmend komplexer und professioneller werden, müssen Attacken frühzeitig erkannt werden. Ein Erkennen ist der **erste Schritt dazu, weitere Angriffe zu verhindern**.

Welche Ansätze zur Erkennung von Cyber Attacken gibt es?

Zwei weit verbreitete Verfahren zur Erkennung von Cyber Attacken sind die **Mustererkennung** und die **Anomalieerkennung**.

Die **Mustererkennung** versucht, Angriffe anhand von **bereits durchgeführten Attacken** und deren Muster zu erkennen. Der wesentliche Nachteil der Mustererkennung besteht darin, dass neuartige Angriffe nicht erkannt werden können.[4]

Bei der **Anomalieerkennung** wird das **übliche Verhalten** des Systems festgehalten. Treten Ereignisse auf, welche von diesem Verhalten abweichen, also eine Anomalie darstellen, liefert dies einen Hinweis auf einen Angriff. Auf diese Weise können auch neuartige Cyber Attacken erkannt werden.[5]

Beispiele für Verfahren zur Anomalieerkennung

Analyse von Dateizugriffen: Die Position eines Dokumentes innerhalb der Ordnerstruktur und die Zugriffe verschiedener Nutzer auf die Datei sind Indikatoren für den Informationsgehalt eines Dokumentes. Jeder Nutzer hat ein übliches Verhalten, das bedeutet, er greift normalerweise auf Dokumente mit ähnlichem Informationsgehalt zu. Weicht der Informationsgehalt eines angefragten Dokumentes von seinem üblichen Verhalten ab, kann dies auf einen Fall von Spionage hindeuten.[6]

Analyse von Log-Dateien: Einzelne Zeichen(ketten) innerhalb von Log-Dateien werden selektiert und ein Muster über diese gebildet (Mustererkennung aus der Bioinformatik). Abweichungen vom üblichen Muster weisen auf Anomalien hin.[7]

Weitere Informationen und Verfahren finden Sie unter: http://bit.ly/2jmWC3g

---

[1] Claudia Eckert: IT-Sicherheit, Konzepte – Verfahren – Protokolle. 8. Auflage, Oldenburg Verlag, München 2013. Seite 20

[2] Vgl. Jeferson W. de Godoy Stênico, Lee L. Ling: Network Traffic Monitoring and Analysis. In: Al-Sakib K. Pathan: The State of the Art in Intrusion Prevention and Detection. Taylor & Francis Group. Boca Raton 2014, S. 23-46.

[3] Vgl. Fußnote 1

[4] Vgl. zum Absatz Jonny Milliken: Introduction to Wireless Intrusion Detection Systems. In: Al-Sakib K. Pathan: The State of the Art in Intrusion Prevention and Detection. Taylor & Francis Group. Boca Raton 2014, S. 335-360.

[5] Vgl. zum Absatz Pedro García-Teodoro, Jesus E. Díaz-Verdejo, Gabriel Maciá-Fernández, Erique Vázquez: Anomaly-based network intrusion detection: Techniques, systems and challenges. In: Computers & Science. Nr. 28, 2009, S. 18-28.

[6] Vgl zum Absatz Christopher Gates, Ninghui Li, Zenglin Xu, Suresh N. Chari, Ian Molloy, Youngja Park: Detecting Insider Information Theft Using Features from File Access Logs. In: Miroslaw Kutylowski, Jaideep Vaidya (Hrsg.): Computer Security – ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part I. Springer-Verlag, Cham, Heidelberg, New York, Dordrecht, London 2014, S. 383-400.

[7] Vgl. zum Absatz Roman Fiedler, Florian Skopik, Thomas Mandl, Kurt Einzinger: Erkennen von Anomalien und Angriffsmustern. In: Cyber Attack Information System. Springer-Verlag, Berlin, Heidelberg 2015, S. 89-118.