DATENBLATT ZENTRALES LOGMANAGEMENT

Leider muss man vermehrt aus den Medien von Unternehmen erfahren, deren IT-Infrastruktur kompromittiert wurde. Infolgedessen werden Daten entwendet beziehungsweise verschlüsselt, die betroffenen Unternehmen erpresst, ihre IT-Infrastruktur gezielt an bestimmten Stellen oder gar komplett zerstört. Ob die Motivation der Angreifer nun aus blinder Zerstörungswut, ideologischer Natur oder finanziellen Interessen heraus motiviert ist, für die betroffenen Unternehmen bedeuten die Folgen leider nicht selten Reputationsverlust, Ermittlungen - je nach eigenem Verschulden in Form versäumter Maßnahmen hinsichtlich IT-Sicherheit - durch die Strafverfolgungsbehörden auch gegen das betroffene Unternehmen selbst und Folgekosten, die mitunter die Existenz des Unternehmens bedrohen können.

Die Angreifer sind dabei leider oft nicht zu identifizieren, schließlich haben sie größtes Interesse daran, ihre Identität zu verschleiern. Deshalb führen sie im Rahmen des Angriffs entsprechende Maßnahmen durch. Eine zentrale und in aller Regel erste Maßnahme ist es deshalb, mögliche Spuren in den Log-Dateien durch deren Löschung oder Änderung zu verwischen. So ist es kaum mehr möglich, im Rahmen der IT-Forensik Identität der Angreifer zu ermitteln und den Ablauf des Angriffs zu rekonstruieren. Gerade die Strafverfolgungsbehörden sind aber auf diese Informationen angewiesen. Die Gewährleistung unkompromittierter Logs wird deshalb von den einschlägigen IT-Versicherungen und durch für das Unternehmen geltende Compliance-Regeln zwingend gefordert.

Wie lässt sich dies aber sicherstellen? Wie können Sie Ihre Logs vor Angreifern schützen und somit Strafzahlungen gegen Ihr Unternehmen oder ausbleibende Versicherungsleistungen infolge der unterlassenen Absicherung Ihrer Logs gegen eine Kompromittierung durch Angreifer verhindern?

Durch die in der INFOSERVE SERVICE CARD PLATIN enthaltene Sicherung Ihrer Log-Dateien befinden sich diese zusätzlich außerhalb Ihrer IT-Infrastruktur zentral in einem der hochgesicherten INFOSERVE Rechenzentren.
Somit ist deren Validität auch nach einem Angriff auf ihre IT-Infrastruktur sichergestellt, und die Logs können somit unter anderem für die forensische Analyse und Beweisführung herangezogen werden.

Zusätzlich können ihre Log-Daten bei uns an zentraler Stelle aggregiert und analysiert werden, um aus der umfassenden, korrelierten Betrachtung von Informationen aus mehreren Quellen gegebenenfalls die entscheidenden Hinweise zu erhalten, die bei der isolierten Betrachtung der einzelnen Logs verborgen blieben.

Natürlich sind diese Möglichkeiten aber nicht nur im Falle eines Cyberangriffs, sondern auch bei der klassischen Fehlersuche äußerst hilfreich.

Unterstützt werden Linux-/Unix- und Windows-Systeme, Router, Switches sowie Firewalls, welche die technischen Voraussetzungen erfüllen. Im Basisumfang ist die Sicherung der üblichen System- beziehungsweise Event-Logs enthalten. Weitreichendere sowie bei Bedarf für Ihre konkreten Anwendungsfälle maßgeschneiderte Lösungen richten wir gerne in Absprache mit Ihnen zu einem von der jeweiligen Lösung abhängigen Mehrpreis ein.