Incident Response für KMUs

Diplomanden

Marco Martinez

Severin Grimm

Einleitung: Kleinere und mittlere Unternehmen (KMUs) investieren viel Geld in die Digitalisierung ihrer Arbeitsprozesse und sind auf ihre digitale Infrastruktur angewiesen. Durch diese Digitalisierung erlangt eine Unternehmung auf dem Markt den wirtschaftlichen Vorteil, der zur Rentabilität nötig ist. Gerade diese Digitalisierung fördert die Attraktivität der KMUs gegenüber Cyberkriminellen. Cyberkriminelle nehmen häufig KMUs ins Visier und scheuen nicht davor zurück, mit gestohlenen oder verschlüsselten Daten hohe Geldsummen zu erpressen. Wer den Forderungen nicht nachkommt, muss zahlreiche Systeme zurücksetzen oder unternehmenskritische Daten werden veröffentlicht. Oftmals erreichen Cyberkriminelle die Unternehmenssyteme durch Sicherheitslücken und bleiben dabei unentdeckt. Diese Angriffe können mit einfachen Massnahmen erschwert und von oft kostenlosen Sicherheitsapplikationen entdeckt werden.

Ziel der Arbeit: Das Ziel dieser Bachelorarbeit ist es, KMUs in der Planung, der Vorbereitung und der Abwicklung von Cyberangriffen zu unterstützen. Die KMUs werden entsprechend ihrer Grösse mit Anleitungen, Vorlagen und Applikationen ausgestattet. Die erarbeiteten Anleitungen und Vorlagen sind praxisnah, für IT-Fachkräfte eines KMUs leicht verständlich und schnell umzusetzen. Das interaktive Incident-Detection-Training festigt das durch die Anleitungen erlernte Fachwissen.

Ergebnis: Die Ergebnisse dieser Bachelorarbeit sind in vier Bereiche aufgeteilt. Es wurden 4 Ergebnisformate gewählt, um eine möglichst breite Hilfestellung bieten zu können.
Anleitungen: Es wurden technische Anleitungen für Sicherheits-‹Best Practices› in mehreren Bereichen erstellt. Diese reichen von konzeptionellen Vorgehensweisen bis hin zu konkreten Implementationen. Ausserdem wurden Anleitungen zur automatischen Installation und Verwendung einer Sicherheitsapplikation erstellt, welche KMUs hilft, Cyberangriffe zu entdecken.
Vorlagen: Es wurden zwei Vorlagen zur Definition der Vorgehensweisen bei einem Cyberangriff erstellt. Die Vorlagen unterstützen KMUs darin, bei einem Cyberangriff effektiver reagieren zu können, da alle Prozessabläufe vorgegeben sind und dadurch Klarheit im Vorgehen herrscht.
Sicherheitsapplikation: Es wurde eine automatische Installation inklusive Installations- und Benutzeranleitung für ein Sicherheitssystem erstellt. Dieses bringt Sichtbarkeit und Transparenz in die IT-Infrastruktur, mit welchem akutelle Ereignisse nachvollzogen werden können. Dadurch können Anomalien in der IT-Infrastruktur entdeckt und es kann darauf reagiert werden.
Incident-Detection-Training: Mit dem Incident-Detection-Training können KMUs ihre IT-Fachkräfte in der Verwendung der Sicherheitsapplikation trainieren. Dies hilft KMUs, Angriffe frühzeitig zu erkennen.

Referentin
Prof. Dr. Nathalie Weiler

Korreferent
Michael Günther, SwissSign Group AG, Uster, ZH

Themengebiet
Sicherheit