IHK Offenbach am Main Stadt und Kreis

Offenbacher Wirtschaft

www.offenbach.ihk.de
11 2015

Saubere Sache

Unternehmensnachfolge aktiv gestalten
▶ S. 25

Wirtschaft braucht Regionaltangente West
▶ S. 28

Schattenseiten der digitalen Welt
▶ S. 40

2,30€

Umdenken zum Schutz vor digitalen Angriffen

Schattenseiten der digitalen Welt

Die fortschreitende Digitalisierung bietet wirtschaftlich ganz offensichtlich auch sehr viele Betätigungsfelder für Kriminelle, denn immer öfter lesen wir Nachrichten wie „Daten gestohlen", „Hackereinbruch", „Online Erpressung" und dergleichen.

Erfolgreiche Angriffe auf Computer diverser Unternehmen, das Kfz-Wunschkennzeichenportal und jüngst sogar den deutschen Bundestag zeigen nur zu deutlich, wie allgegenwärtig die Schattenseiten der digitalen Welt sind.

Während Großkonzerne schon jahrelang im Fokus stehen und sich entsprechend gerüstet haben, sind Angriffe auf mittelständische Unternehmen in den letzten Jahren massiv angestiegen und treffen häufig auf unzureichend vorbereitete Ziele.

Zum einen wird speziell versucht, Forschungs- und Entwicklungsergebnisse abzugreifen, zum anderen, unmittelbaren finanziellen Gewinn zu erzielen. Erst kürzlich wurde wieder in einem Unternehmen der elektronische Rechnungsversand erfolgreich manipuliert, so dass als Bankverbindung ein Konto der Angreifer ausgewiesen wurde, natürlich samt dem freundlichen Hinweis, man möge bitte die neue Kontoverbindung beachten.

Sorgloser Umgang mit Dienstgeräten ist ein Einfallstor für Cyber-Kriminelle. Foto: Pixelio

Elektronische Erpressungen gehören mittlerweile auch zum Alltagsgeschäft. Diese Angriffe richten sich einerseits gegen Unternehmen, die zuvor zielgerichtet ausgekundschaftet wurden. Andererseits gegen jegliche Systeme, die den Kriminellen aufgrund unzureichender Schutzmaßnahmen ‚einfach so' ins Netz gehen. In der Folge werden dann beispielsweise wichtige Dokumente auf der Festplatte verschlüsselt. Um wieder an die eigenen Daten zu kommen, müssen die Opfer nun Lösegeld zahlen, in aller Regel in Bitcoins, virtuelle Währung im Internet, die anonymes Bezahlen ermöglicht. Durch regelmäßige Updates, aktuell gehaltene Software samt Virenscanner und Inhaltsfilter vermag viele dieser Schädlinge abzuhalten. Im schlimmsten Fall wären verlorene Daten zumindest aus einem funktionierenden Backup wieder herzustellen.

Als weitere Bedrohung hat mittlerweile die Erpressung mittels „Denial-of-Service" Einzug gehalten. Hierbei wird dem Opfer angedroht und auch demonstriert, dass es möglich wäre, die IT-Infrastruktur lahmzulegen und nur gegen eine Schutzgebühr davon Abstand genommen wird. Aufgrund nicht implementierter Erkennungs- und Abwehrmöglichkeiten haben hier schon einige Unternehmen Lehrgeld zahlen müssen.

Durch mangelhafte Trennung zwischen Büronetzwerken und Produktionssystemen erlangen Angreifer oftmals sehr einfach Zugriff auf Steuerungssysteme und die darauf befindlichen sensiblen Daten. Besonders im Hinblick auf die kommende weitere Vernetzung im Rahmen von Industrie 4.0 sollte dies unbedingt beachtet werden.

Weiterhin verlieren immer noch viele Unternehmen sensible und unternehmenskritische Daten, weil diese gesammelt auf der Notebookfestplatte liegen. Mitnehmen sollte man nur das, was vor Ort unbedingt benötigt wird. Als Mindestschutz gilt hierfür eine Vollverschlüsselung der Festplatte, Sperrung von USB Anschlüssen und der Einsatz starker Passwörter.

Ein weiterer Angriffspunkt sind die eigenen Mitarbeiter, die mittels so genanntem „Social-Engineering" für einen weitergehenden Angriff missbraucht werden, ohne dies selbst bemerken zu können. Durch geschicktes Zuspielen von „Malware", beispielsweise in fingierten E-Mails, erlangen die Angreifer Zugriff auf deren Rechner, um mit den Zugriffsrechten des Mitarbeiters dann weitergehend auf Daten, Server und Applikationen

zuzufassen. Aufklärung und Schulungsmaßnahmen stärken die Erkennungsmöglichkeiten des Mitarbeiters.

Besonders besorgniserregend ist die Tatsache, dass die meisten Unternehmen einen Fremdzugriff oder Missbrauch ihrer IT-Systeme erst nach Monaten bemerken, viele sogar erst durch eine Meldung von Dritten.

Durch eine sorgfältige Auswertung von Nutzungsprotokollen und den systemeigenen Logmeldungen könnte oftmals ein Missbrauch frühzeitig erkannt werden, denn meist finden sich hier passende Hinweise auf schädliches Treiben. Solche Lösungen sind sogar mit etwas Vorbereitung und Abstimmung datenschutzkonform einsetzbar.

Einigkeit herrscht darüber, dass mit Firewall und Virenscanner alleine kein ausreichender Schutz mehr gegeben ist. Je nach Schutzbedarf der einzelnen Systeme und Daten gehören spezielle Inhaltsfilter und „Malware"-Analysesysteme als zusätzliche Filterstufe dazu.

Eine strikte Netzwerktrennung innerhalb der einzelnen Unternehmensbereiche bis hin zur völligen Abschottung wichtiger Systeme vom Internet erschwert zwar manchmal das Arbeiten, bietet aber einen deutlichen Zugewinn beim Schutz. Der Einsatz von Verschlüsselung für Datenträger und Kommunikationswege ist noch viel zu selten Standard. Ebenso sollten veraltete Anmeldeprozeduren mit simplen Passwörtern durch sicherere Verfahren mit Zweifaktorauthentifizierung und Einmalpasswörtern ersetzt werden.

Um diese und weitere Maßnahmen zielgerichtet umsetzen zu können, ist die Inventarisierung von Informationswerten und Bewertung hinsichtlich der Bedeutung für das Unternehmen grundlegende Voraussetzung. Darauf aufbauend können Sicherheitsleitlinien, Zugriffsrechte, technische Regelungen und weitere Schutzkonzepte aufgebaut und regelmäßig auf Wirksamkeit überprüft werden.

Die kriminellen Kräfte nutzen das gesamte Arsenal, um an die Daten und letztendlich das Geld des wirtschaftsstarken Mittelstandes zu kommen. Nur wer sich mit den passenden Mitteln und Verfahren dagegen zur Wehr setzt, wird auch in Zukunft mit ausschließlich positiver Presse aufwarten können.

Autor:
Christian Schülke
Inhaber schuelke.net – internet.security.consulting, Langen
Telefon (06103) 5715571
E-Mail cs@schuelke.net