Informationen über die Maßnahmen, mit denen die Stadtwerke Baden-Baden auf Sicherheits- und Integritätsverletzungen sowie auf Bedrohungen und Schwachstellen in ihren Systemen reagieren

1. Allgemeines

Die Sicherheit im Zusammenhang mit der Lieferung der Telekommunikations- und Entertainmentdienste sind uns ein sehr großes Anliegen. Wir bauen dabei auf zwei starke Säulen. Mit dem Einsatz der neusten Technologien sorgen wir bereits für ein sehr hohes Sicherheitsniveau. Darüber hinaus haben wir verschiedenste organisatorische Maßnahmen implementiert, um das Sicherheitsniveau noch weiter zu steigern.

Der größte Teil unserer Maßnahmen zielt allerdings ausschließlich auf die Systeme, mit denen wir unsere Kunden beliefern. Der Kunde sollte auch in seinem Verantwortungsbereich weitere Maßnahmen zur Erhöhung der IT-Sicherheit treffen. Dazu gehören z. B. technische Maßnahmen wie eine lokale Firewall sowie ein aktueller Virenschutz. Wichtig sind aber auch ein gutes Know-how über die Gefahren im Internet. So sollte z. B. keine E-Mail von einem unbekannten Absender geöffnet werden.

Die Zertifizierungsstelle der TÜV SÜD Management Service GmbH bescheinigt uns regelmäßig im Rahmen von Audits, dass unser Informationssicherheits-Managementsystem (ISMS) im Geltungsbereich „Sicherer Betrieb der Steuerungs-, Überwachungs- und Prozessleittechnik des Strom- und Gasnetzes“ die Anforderungen des IT-Sicherheitskatalogs gem. §11 Abs. 1a EnWG (08/2015) erfüllt. Für den Bereich Telekommunikations- und Multimediadienste haben wir unser ISMS um ein TK-Sicherheitskonzept erweitert, das der Bundesnetzagentur (BNetzA) regelmäßig zur Prüfung und Abnahme vorgelegt wird.

2. Technische Maßnahmen

Der Internetzugang ist für unsere Kunden transparent. Das bedeutet, dass sich keinerlei Sicherheitstechnik zwischen dem Kundenrouter und dem Internet befinden. Daher sollten die Sicherheitsmechanismen auf dem Router des Kunden auf keinen Fall deaktiviert werden. Zudem sollten neue Updates umgehend durch den Kunden installiert werden.

Alle wichtigen zentralen Systeme der Stadtwerke sind redundant ausgelegt und werden in zwei ebenfalls redundanten Rechenzentren vorgehalten. Beide Rechenzentren verfügen über einen Zutritts- und Gebäudeschutz. So können die Rechenzentren ausschließlich von autorisiertem Personal betreten werden. Zudem wird ein Einbruch oder ein Brand sofort detektiert und an unsere zentrale Netzführung bzw. die Feuerwehr übertragen. Durch entsprechende Techniken können Brände bereits während der Entstehung gelöscht werden. Beide Rechenzentren verfügen über eine Klimatisierung sowie eine USV und Notstromversorgung, so dass wir den Betrieb auch während eines Stromausfalls aufrechterhalten können. Die beiden Rechenzentren sind redundant über zwei unterschiedliche Netzprovider nach Stuttgart und Frankfurt an das Internet angeschlossen. Für die Absicherung der TV-Versorgung wurde ein zusätzlicher lokaler Parabolspiegel installiert, der beim Ausfall der TV-Lieferung durch den Vorlieferanten zumindest die wichtigsten 120 Programme weiterhin zur Verfügung stellt. Die Anbindung der Telefonie erfolgt ebenfalls redundant nach Stuttgart und Frankfurt über – von der Internetanbindung – separierte Leitungen, um die Sprachqualität sicherzustellen.

Die Anbindung der Router der Kunden erfolgt über einen verschlüsselten PPPoE-Tunnel zu unseren zentralen Internetroutern. Ein gegenseitiger Zugriff wird damit ausgeschlossen. Alle zentralen Serversysteme der Stadtwerke sind über ein zweistufiges Firewall-Konzept an das Internet angeschlossen. Alle Server, die über einen Reverse-Proxyserver aus dem Internet erreichbar sind, wurden zusätzlich gehärtet, um die Sicherheit noch weiter zu erhöhen.

3. Organisatorische Maßnahmen

Die getroffenen organisatorischen Maßnahmen sind für die Stadtwerke mindestens genauso wichtig wie die technischen Maßnahmen. Als Betreiber kritischer Infrastrukturen haben die Stadtwerke bereits vor einigen Jahren ein Informationssicherheitsmanagementsystem eingeführt. Dabei ist das oberste Ziel, die Sicherheit immer wieder zu hinterfragen, neue Risiken zu erkennen, zu bearbeiten und zu beseitigen. Auf diese Weise beschreiten wir einen kontinuierlichen Verbesserungsprozess, den wir regelmäßig gegenüber einem externen Auditor nachweisen müssen, um unser Sicherheitszertifikat auch in Zukunft als Nachweis unseres hohen Sicherheitsstanddards zu behalten.

Wir bedienen uns der Meldungen des Bundesamts für Sicherheit in der Informationstechnik und werden so über Schwachstellen in Systemen frühzeitig informiert. Anschließend untersuchen wir, ob eine gemeldete Schwachstelle für uns relevant ist und treffen die erforderlichen Maßnahmen.

Zusätzlich werden sicherheitskritische Updates der Hersteller umgehend installiert, um bekannte Schwachstellen von vornherein zu schließen.

Die größten Gefahren im Internet gehen von den Nutzern aus. Daher werden unsere Mitarbeiter für das Thema IT-Sicherheit besonders geschult und immer wieder sensibilisiert. Mit dieser Maßnahme können wir die Sicherheit noch einmal wesentlich erhöhen.

Unser IT-Sicherheitsbeauftragter hat die Aufgabe, die technischen Systeme und die organisatorischen Maßnahmen regelmäßig zu prüfen und zu hinterfragen. Die daraus gewonnenen Erkenntnisse fließen wiederum in den Verbesserungsprozess ein und helfen, die Sicherheit zu erhöhen oder zumindest auf einem gleichbleibend hohen Stand zu halten.

Bei allen getroffenen Maßnahmen verbleibt immer ein Restrisiko, das nicht mehr weiter minimiert werden kann. Sollte eine solches Restrisiko – im unwahrscheinlichsten Fall – doch einmal eintreten, sind entsprechende Prozesse implementiert, um die Auswirkungen zu minimieren oder bestenfalls auszuschließen.

Mit all diesen Maßnahmen sind die Stadtwerke Baden-Baden den Anforderungen eines Internetserviceproviders sehr gut gewachsen. Nur so können wir unseren Kunden ein sicheres und hochverfügbares Angebot liefern.

Baden-Baden, den 15.06.2020