terreActive AG
Kasinostrasse 30
5001 Aarau

Fon 062 834 00 55
Fax 062 823 93 56

www.security.ch
contact@terreActive.ch

Kundeninformation von terreActive zur IT-Sicherheit in der öffentlichen Verwaltung

Aarau, 20.07.2016. Erpressungen von Cyberkriminellen machen Schlagzeilen. Auch öffentliche Verwaltungen bleiben von Attacken nicht verschont. Das bringt sie in Bedrängnis, denn der Schutz einer Gemeinde-IT ist anspruchsvoll. Wo beginnen? Welcher Schutz ist sinnvoll?

Cyberattacken treffen heutzutage alle: Zeitungen, Online-Shops und sogar weltweite Zahlungsdienstleister. Gemeindeverwaltungen und Städte sind noch stärker gefordert als die Privatwirtschaft. Denn der systematische Schutz ihrer IT ist – selbst für kleine Gemeinden – kompliziert.

Heterogenität von Gemeinden macht Schutz aufwendig

Das hat mehrere Gründe. Erstens sind öffentliche Verwaltungen sehr heterogene Gebilde. Ihre IT dient verschiedenen Anwendern: Je nach Departement und Funktion variieren Kenntnisstand und Anforderungen. Die Steuerbehörde beispielsweise will maximale Sicherheit, Schulen wollen maximale Flexibilität.
Zweitens bringt die Heterogenität eine Vielzahl verschiedener Anwendungen und Daten mit sich. Nicht alle diese Daten benötigen den gleichen Schutz. Auf manche Daten wird eine Gemeinde im schlimmsten Fall während ein paar Tagen verzichten können – bis sie vom Backup wiederhergestellt sind. Bei anderen kann dies weitreichende Folgen haben, finanzielle und rechtliche.

Grosse Hürden für kleine Gemeinden

Die Sicherheitsanforderungen für alle Daten zu definieren, ist selbst in kleinen Gemeinden eine Herkulesaufgabe. Den gleichen Schutz für alle Daten und Anwendungen anzuwenden ist keine Lösung. Denn dann werden die Schutzmechanismen zu kompliziert und behindern womöglich die Arbeit im Alltag. Vor allem für kleine Gemeinden ein Dilemma: Ihre IT zu schützen ist so komplex und aufwendig wie bei einer grossen Verwaltung, nur stehen ihnen dafür kaum Ressourcen und Know-how zur Verfügung. Schützenswerte Daten gibt es in jeder Gemeinde, davon ausgenommen ist also niemand.

Gefahren: DDoS-Attacken und Ransomware

Nicht jede Gemeinde ist gleich gefährdet: Je kleiner die mögliche Beute, desto kleiner der Aufwand, den Angreifer bereit sind zu erbringen. Die grösste Gefahr sind deshalb banale Angriffsformen wie DDoS-Attacken oder Ransomware. Bei DDoS werden Systeme lahmgelegt, indem sie vom Angreifer mit Anfragen bombardiert werden. Ransomware ist Schadsoftware, die auf Rechner eingeschleust wird und welche die ganze IT lahmlegt oder Daten verschlüsselt. Für die Entschlüsselung fordern die Angreifer Lösegeld. Vertrauliche Daten gelangen dadurch zwar nicht in falsche Hände, die Folgen sind trotzdem ärgerlich, zeit- und kostspielig: Mitarbeiter können nicht mehr auf Daten zugreifen, Einwohner können online keine Formulare oder Auszüge bestellen und bei der Wiederherstellung von Daten geht viel Zeit verloren.

terreActive AG
Kasinostrasse 30
5001 Aarau
Fon 062 834 00 55
Fax 062 823 93 56
www.security.ch
contact@terreActive.ch

Gerade für Ransomware sind Gemeindeverwaltungen beliebte Ziele, und bis heute sind nur wenige darauf vorbereitet. Angreifbar sind alle öffentlich zugänglichen Dienste wie die Website oder das E-Gouvernement-Portal, aber auch interne Systeme wie Mail- und File-Server.

Vor allem grössere Gemeinden oder Stadtverwaltungen können auch Ziel werden von Advanced Persistent Threats (APT). Das sind Angriffe, die sich über einen längeren Zeitraum erstrecken und deshalb schwer erkennbar sind. Angreifer gehen dabei gezielt behutsam vor, um jede Aufmerksamkeit zu vermeiden. Solche Angriffe sind sehr aufwendig und teuer, sie kommen nur zum Einsatz, wenn eine entsprechend grosse Beute zu erwarten ist.

Erster Schritt: Daten-Inventar und Audit

Wo beginnen, ohne sich in Details zu verlieren? Als erstes muss sich die Gemeinde bewusst werden, über welche Daten sie verfügt. Ein solches Daten-Inventar ist die Basis für eine Standortbestimmung, die in Form eines Security Assessments (Audits) gemeinsam mit einem Security-Dienstleister durchgeführt werden kann: Hier werden schützenswerte Daten, die Risiken und ihre Eintrittswahrscheinlichkeit detailliert aufgeführt.

Schutz aufbauen

Je nach Risikoprofil und Eintrittswahrscheinlichkeit kann eine Gemeinde damit beginnen, Anwendungen und Daten zu klassifizieren. Erst danach kann ein Security-Anbieter gezielte Schutzmassnahmen aufbauen. Diese reichen von Virenschutz-Software über Firewalls bis zu Netzwerksegmentierung – also der technischen und organisatorischen Trennung von Applikationen. Auf diese Weise kann verhindert werden, dass unkritische und weniger geschützte Applikationen die kritischen gefährden.

Einbrüche erkennen

Genauso wichtig wie der Schutz vor Cyber-Attacken ist, solche überhaupt zu erkennen. Denn Cyberkriminelle entwickeln ihre Angriffe weiter und finden schnell neue, noch ungesicherte Lücken. Die Schutzmassnahmen sind im Idealfall also im Einklang mit Massnahmen zur Erkennung und Nachverfolgung von Angriffen und Einbrüchen. Es ist wie beim Schutz von Gebäuden: Überwachungskameras und Alarmanlage sind ebenso wichtig wie Sicherheitstüren und Stacheldraht. Für die Erkennung von Angriffen haben sich drei Typen von Systemen bewährt, die auch kombiniert werden können:

- *Network-Intrusion-Detection* erkennt bekannte Angriffe.
- *Log-Management-Systeme* zeichnen Aktivitäten auf und dienen als Grundlage für Nachforschungen oder Security Monitoring (siehe Box «SecMon»).
- *Threat-Detection-Lösungen* analysieren das Verhalten der IT und decken Unregelmässigkeiten auf.

Wissen schützt

Technische Massnahmen sind aber nur ein Teil eines wirksamen Schutzes. Am besten gewappnet sind Organisationen, die sich selber Wissen aneignen über Cyber-Attacken. Zentral ist dabei, Muster in Daten richtig zu interpretieren und Anzeichen von Attacken zu erkennen. Öffentliche Verwaltungen ohne eigene IT-Abteilung sollen sich also von ihrem IT-Anbieter beraten lassen – nicht nur für die Implementation von Schutzmassnahmen, sondern auch für den sicheren Betrieb ihrer Anwendungen im Alltag (siehe Box «Sicherheitsfragen»).

terreActive AG
Kasinostrasse 30
5001 Aarau

Fon 062 834 00 55
Fax 062 823 93 56

www.security.ch
contact@terreActive.ch

Infobox SecMon

Was ist Security Monitoring?

Security Monitoring bezeichnet den permanenten Prozess vom Sammeln und Analysieren von Hinweisen und Warnungen zur IT-Sicherheit. Es hat zum Ziel, Bedrohungen zu entdecken, zu verfolgen und darauf zu reagieren. Security Monitoring ist eine Aufgabe des Security Operations Centers (SOC). IT-Security-Anbieter oder grosse Firmen betreiben SOCs, um sämtliche sicherheitsrelevanten Prozesse und Aufgaben zu organisieren. Es besteht aus einem Team von Security Engineers (CERT, Computer Emergency Response Teams).

Infobox Sicherheitsfragen

Mit diesen Fragen erhalten Gemeindebehörden einen ersten Eindruck über den Stand Ihrer IT-Sicherheit:

Checklist für den Alltag

- Ist der Virenschutz auf dem aktuellsten Stand?
- Sind die aktuellsten Updates für alle Programme installiert?
- Ist die IT auf Sicherheitslücken geprüft worden (Vulnerability Scan)?
- Gibt es ein laufendes Backup?
- Ist der Prozess für Backup- und Wiederherstellung erprobt?
- Ist der Zugriff auf Backups garantiert/geregelt?
- Ist die Erreichbarkeit der IT-Verantwortlichen geregelt?
- Wann wurde das letzte Mal ein Audit durchgeführt?

Fragen an den IT-Verantwortlichen/externen IT-Dienstleister

- Sind die Gemeinde-Daten klassifiziert?
- Gibt es ein Sicherheitskonzept? Sind die Massnahmen dokumentiert? Kann das Sicherheitskonzept ausgehändigt werden?
- Verfügt der IT-Betreiber (Hoster, Security-Anbieter) über eine Zertifizierung nach ISO 27001? (Garantiert Sicherheitsmassnahmen und deren Dokumentation)
- Welche Garantien sind im Service Level Agreement (SLA) vereinbart? Gibt es ein Recht auf externe Security-Audits?
- Kann der IT-Verantwortliche auf Monitoring- und Log-Daten direkt zugreifen?