AG KRITIS

Stellungnahme für die Anhörung des Landtags Nordrhein-Westfalen

Kommunale IT-Sicherheit sicherstellen – Aufbau eines zentralen Kommunal-CERT am 24.06.2021

Manuel Atug

Gründer und Sprecher der AG KRITIS

Der Sachverständige dankt allen ehrenamtlich tätigen ExpertInnen und den vielen SicherheitsforscherInnen aus der AG KRITIS, der erweiterten Community und im Speziellen bei Tim Goos für die Unterstützung.

Kontakt

Manuel Atug

E-Mail: honkhase@ag.kritis.info

Twitter: @HonkHase

Webseite: https://ag.kritis.info

Nachfolgend werden die sechs wesentlichsten Fragestellungen aus Sicht des Sachverständigen dargelegt und auf jeden einzelnen Punkt entsprechend eingegangen.

PERSONAL

Arbeitskräfte im Bereich Informationstechnik sind aufgrund der fortschreitenden Digitalisierung sehr gefragt aber „Mangelware“.

Diese Situation wird sich aufgrund der Bildungspolitik auch in den nächsten Jahren nicht wesentlich ändern, da wir zwar in einer Informationsgesellschaft angekommen sind, aber kein ausreichend angepasstes informationstechnisches und medienkompetentes Wissen in die schulische Ausbildung integriert ist.

Somit ist es weiterhin schwierig bleiben, qualifiziertes Personal für CERTs zu finden. Der Boom in der IT-Sicherheitsbranche erschwert die Bedingungen zusätzlich. Ohne ausreichend qualifiziertes Personal können die Tätigkeiten eines CERTs allerdings nicht ohne weiteres vorgenommen werden. Folglich müssen entsprechende Anreize geschaffen werden, um benötigtes Fachpersonal zu gewinnen und fortlaufend weiterzubilden. Hier ergeben sich allerdings große Schwierigkeiten für Kommunalverwaltungen. Durch die große Nachfrage und den oben beschriebenen Engpass auf absehbare Zeit sind die Gehälter im Bereich IT-Sicherheit gestiegen. Der öffentliche Dienst kann auf kommunaler Ebene nicht mit der freien Wirtschaft konkurrieren.

Insbesondere die Gehaltsniveaus für leitende Positionen im Bereich der IT-Sicherheit, bei denen das durchschnittliche Jahresbruttogehalt bereits in 2016 bei 109.694,- €[1] lag, sind von den vorhandenen Entgeltgruppen nicht abbildbar. Darüber hinaus werden oft nicht-monetäre Leistungen wie Dienstwagen oder flexible Remote-Work als weitere Anreize zur Personalgewinnung angeboten. Zusätzlich muss Fachpersonal für CERTs, besonders in den ersten Jahren, umfassend auf den speziellen Einsatzgebieten geschult werden. Die Kosten für diese Fachschulungen liegen weit über dem Durchschnitt von 50,- € pro Mitarbeiterin und Jahr des Kostenansatzes der KGSt vom Jahr 2018/2019[2].

In der freien Wirtschaft ist es üblich, IT-Sicherheits-Fachpersonal jedes Jahr auf mehrere Fachtagungen, Weiterbildungen und Konferenzen zu entsenden, um das Wissen dieser ExpertInnen aktuell zu halten – die Kosten dafür sind im Regelfall pro Mitarbeiter größer als 10.000,- € pro Jahr. Oft bewegen sich die Kosten für ein einzelnes Ticket einer relevanten Fachveranstaltung schon zwischen 500,- € und 2000,- €, ohne das Reisekosten oder Unterkunft berücksichtigt wurden.

Insgesamt zeigt sich, dass viele einzelne Kommunalverwaltungen nicht in der Lage sein werden, das nötige Fachpersonal zu finden oder einzustellen. Daher sollten die Kommunalverwaltungen lieber ein Pooling betreiben, um die Kosten aufzuteilen und dem Mangel entgegenzuwirken. Dieses Prinzip wird auch in der Wirtschaft angewandt und ist im Bereich der IT-Sicherheit üblich, da identische IT-Sicherheitsvorfälle bei einer Anwendungsart oder einem Betriebssystemtyp in der gleichen Kommune in der Regel nicht mehrfach auftreten. Wohl aber ist es realistisch, dass dieser Vorfall bei mehreren Kommunen vorkommen kann.

[1] https://www.faz.net/aktuell/karriere-hochschule/recht-und-gehalt/it-sicherheitsleute-bekommen-immer-bessere-gehaelter-14125914.html
[2] Vgl. KGSt®-Bericht 9/2018: Kosten eines Arbeitsplatzes (Stand 2018/2019), S. 34

KOMMUNEN ALS ESSENTIELLE DIENSTLEISTER

Die Kommunalverwaltungen speichern viele personenbezogene und damit sensitive Informationen und Details der BürgerInnen. Diese Informationen sind oftmals höchst vertraulich, da sie ein umfassendes Bild zu jeder Bürgerin liefern können und deren Verlust, Abgriff oder auch Veröffentlichung einem Verlust der Identität, Benachteiligungen und sogar zu einer Gefahr für Leib und Leben werden kann. Die Sicherheit dieser Daten liegt in der Verantwortung der Kommunen und unterliegt keinen direkten gesetzlichen Auflagen oder Sanktionierungen. Solange noch kein Schaden eingetreten ist, dominiert unserer Ansicht nach die Wahrnehmung, dass an IT-Sicherheit gespart werden kann, da die Budgets ohnehin schon zu schmal sind. Nach Aussage des BMI nehmen die Cyberangriffe auf politische Ziele, also auch den Staat und die Verwaltung und damit auch auf die kommunalen Verwaltung, stetig zu[3]. Die zunehmend stattfindenden Ransomwarevorfälle in kommunalen IT-Systemen verstärken das Problem erheblich. Die Bedrohungslage schätzen wir als kritisch ein.

Diese Situation muss auch vor dem Hintergrund der Wahlen betrachtet werden, da diese von den Kommunen ausgerichtet werden. Es ist zu erwarten, dass politisch motivierte Akteure verstärkt versuchen werden, Einfluss auf die Wahlen auszuüben.

BürgerInnen müssen darüber hinaus befürchten, dass ihre hochvertraulichen Daten im Rahmen von erfolgreichen Ransomwareangriffen abgegriffen und veröffentlicht werden.

Um die Sicherheit der Daten und Dienstleistungen der Kommunen zu gewährleisten, ist ein kommunales CERT sinnvoll. So würde durch dieses die kommunale Infrastruktur auf Schwachstellen geprüft werden und Mindest-Sicherheitsstandards eingeführt werden. Zudem kann ein CERT die Anpassung an die sich schnell ändernden Gegebenheiten in der IT-Sicherheit koordinieren und notwendige Maßnahmen landesweit priorisieren.

[3] https://www.bmi.bund.de/DE/themen/sicherheit/spionageabwehr-wirtschafts-und-geheimschutz/cyberspionage/cyberspionage-artikel.html

GESETZLICHE VORSCHRIFT ZUR TEILNAHME

IT-Sicherheit wird gerne vernachlässigt. Dies liegt an den schwer zu messenden Leistungen, denn eine funktionierende IT-Sicherheit glänzt durch ausbleibende Sicherheitsvorfälle. Diese können aber auch aus anderen Gründen ausbleiben. So zeigen sich Einsparungen erst, wenn ein Vorfall eintritt. Um dem vorzubeugen, sollten die Kommunen einen gemeinsamen CERT Betrieb aufsetzen, an dem alle Kommunen teilnehmen, da er nicht optional ist.

Die Kosten für das Betreiben des CERTs würden dann gemeinsam von allen Kommunen getragen werden. Je nach lokal vorhandenem Sicherheitsstandard ist zwar von einer Zunahme der Kosten für IT-Sicherheit auszugehen, durch die Bündelung der Ressourcen eines CERTs ist diese Zunahme aber immerhin nicht übermäßig groß. Auch wenn die Kosten des Betriebs eines CERTs auf alle Kommunen umgelegt werden, so ist trotzdem davon auszugehen, dass die vom CERT identifizierten notwendigen Maßnahmen weitere Kosten nach sich ziehen.

Weiterhin kann die Investition in ein CERT die kommunale Verwaltung vor Angriffen durch Ransomware schützen. Damit sinkt die Wahrscheinlichkeit, dass eine kommunale Verwaltung Ransomware-Lösegelder zahlen muss.

Es sollten lieber die geschätzten Gesamtkosten von drei Millionen € jährlich[4] investiert werden, die im laufenden Betrieb eines kommunalen CERTs anfallen, als die selbe Höhe an Mittel als Lösegeld zu bezahlen - und das womöglich mehrfach bei verschiedenen Kommunen. Die Cyberkriminalität und die damit verbundene Anzahl an Vorfällen steigt. Damit steigt auch die Wahrscheinlichkeit, dass Kommunen Opfer von erfolgreichen Cyberangriffen werden. Der Aufbau eines Kommunal-CERTs ist daher als Investition in die IT-Absicherung der Zukunft zu verstehen.

Dies kann allerdings nur gelingen, wenn alle Kommunen bei der Beteiligung am kommunalen CERT mitmachen – eine entsprechende Verpflichtung halten wir für zielführend.

Zusammenfassend wäre eine gesetzliche Vorschrift zur verpflichtenden Teilnahme an einem Kommunal CERT hilfreich, um den Ausbau der IT-Sicherheit bei allen Kommunen gleichermaßen sicherzustellen und damit zukünftige Kosten in Form von Lösegeldern einzusparen.

VERNETZUNG

Ein wichtiger Bestandteil für ein funktionierendes CERT ist die Vernetzung mit anderen Behörden und CERTs. So können gewonnenes Wissen und Erfahrungen geteilt werden, als auch auf mögliche SpezialistInnen und fachliche Expertise zurückgegriffen werden. Der Austausch von Wissen ist essentiell für die IT-Sicherheit, da nur so gegen alle Angriffsvektoren vorgegangen und Abwehrmaßnahmen ergriffen werden können. Dies entspricht auch dem Vorgehen und den Erfahrungen vom Verwaltungs-CERT-Verbund, in dem sich die Länder-CERTs koordinieren.

Diese übergreifende Koordinierung sorgt dafür, dass eine einmal geschlossene Schwachstelle danach in allen kommunalen Verwaltungen gleichermaßen geschlossen werden kann. Unterbleibt der fachliche Austausch zwischen den verschiedenen CERTs, wird es AngreiferInnen erleichtert, eine einmal gefundene Schwachstelle gleich in mehreren Kommunen auszunutzen.

[4] Vgl. Konzeption für ein Kommunal-CERT für Nordrhein-Westfalen v1.02 S. 51

Es erscheint unmöglich, dass ein einzelnes CERT einer Kommune ExpertInnen für alle möglichen Sicherheitsvorfälle vorhält. Möglicherweise gibt es auch bereits entsprechende ExpertInnen in anderen Behörden, so dass Kosten durch die Einsparung von Doppelbesetzungen gespart werden können. Dies setzt allerdings voraus, dass durch Umstrukturierung die knappen Ressourcen des vorhandenen Fachpersonals auch Behördenübergreifend eingesetzt werden können.

Empfohlen wird bei Gründung eines Kommunal CERT priorisierend zuerst die Vernetzung zwischen dem neuen und den bestehenden kommunalen CERTs und anschließend mit dem Landes-CERT. So wird schrittweise ein regionaler Standard aufgebaut und durch den Austausch erhält das Landes-CERT Informationen zu den einzelnen Kommunen. Ohne ein kommunales CERT ist das Landes-CERT nur für die Landesbehörden zuständig und hat keinen Einfluss auf oder Einblick in die Kommunen.

Die besondere Rolle der kommunalen IT-Dienstleister darf beim Aspekt der Vernetzung nicht übersehen werden. Falls es zu einem IT-Sicherheitsvorfall kommt, so ist davon auszugehen, dass der Einsatzort in vielen Fällen innerhalb der Infrastruktur der kommunalen IT-Dienstleister liegen wird. Auch sind die Protokolldaten der kommunalen IT-Dienstleister eine wichtige Datenquelle zum Auswerten von Angriffen und ihren Auswirkungen.

Eine Einbindung der Experten der kommunalen IT-Dienstleister, aber auch eine Rechtsgrundlage für ein kommunales CERT, um überhaupt in der Infrastruktur eines IT-Dienstleisters aktiv werden zu dürfen, ist hier notwendig.

SCHUTZ DURCH KOMMUNAL-CERT

Ein kommunales CERT kann dafür sorgen, dass der Ausfall der IT nach einem Cyberangriff verkürzt wird und die Wiederinbetriebnahme der IT früher erfolgen kann. Auch kann ein kommunales CERT präventiv die IT-Sicherheit verbessern und so erfolgreiche Angriffe unwahrscheinlicher machen.

Durch Schwachstellen-Scanning, die Durchführung von Penetrationstests und durch die Beratung in Bezug auf Best-Practices und zum aktuellen Stand der Technik kann die kommunale IT-Infrastruktur in Bezug auf Resilienz und IT-Sicherheit stetig verbessert werden, wenn genügend Mittel bereitgestellt werden, dass empfohlene Maßnahmen sowohl auf Seiten der kommunalen Verwaltung als auch in der Infrastruktur der kommunalen IT-Dienstleister auch umgesetzt werden.

Sollte trotzdem ein Vorfall auftreten, bietet ein CERT Unterstützung mit geeigneten Fachkräften als First Responder, bei der Aufklärung und Koordination, sowie in der Durchführung einer technischen Analyse (Forensik). Dazu müssen entsprechende Teams aufgebaut bzw. in Kooperationen mit anderen CERTs oder Organisationen zur Verfügung gestellt werden.

Um Kommunen und Organisationen für solche Fälle vorzubereiten, bietet ein CERT Fachschulungen an, welche als kostenpflichtige Leistungen wahrgenommen werden können. Der größte Angriffspunkt bleibt aber der Mensch, weshalb ein CERT auch die Sensibilisierung von MitarbeiterInnen, Verantwortlichen und den Umsetzern durchführen sollte. Rechtliche Fragestellungen und ein Bewusstsein für Informationssicherheit müssen fortlaufend verstärkt werden. Nur so kann langfristig Resilienz gegen Cyberkriminalität aufgebaut werden.

Zuletzt sammelt ein Warn- und Informationsdienst des CERTs alle Informationen zu Schwachstellen, entweder selbst gefunden oder von Drittanbietern und der Community der SicherheitsforscherInnen, und gibt entsprechende Empfehlungen zum Umgang sowie der Behebung dieser an die Kommunen weiter.

KOSTEN

Das hier beschriebene Vorgehen und die errechneten geschätzten Kosten beziehen sich auf den von Christopher Johansson und Thomas Stasch entworfenen Vorschlag eines Konzepts für ein Kommunal-CERT für NRW[5].

Der Aufbau des CERTs wird in drei Phasen unterteilt.

Phase 1 ist die Aufbauphase. In dieser müssen alle nötigen rechtlichen und vertraglichen Rahmenbedingungen geklärt, sowie die Beschaffung und Einführung von benötigter Software durchgeführt werden. Außerdem werden sieben Arbeitskräfte benötigt, die mit dem Aufbau des CERTs beginnen. Um bereits während des Aufbaus Hilfestellungen bei Vorfällen geben zu können sollten Verträge mit externen Dienstleistern geschlossen werden. Insgesamt ist mit Kosten von ca. 1,7 – 1,8 Millionen € pro Jahr zu rechnen, so dass bei 396 Kommunen in NRW ca. 4.400,- € pro Kommune anfällt.

In Phase 2 ist der Aufbau abgeschlossen. Um in den Regelbetrieb überzugehen, müssen die Dienste des CERTs ausgebaut und dafür vier weitere benötigte Arbeitskräfte angestellt werden. Dadurch steigen die jährlichen kosten auf ca. 2,1 Millionen Euro pro Jahr, was ca. 5.200,- € pro Kommune entspricht.

Schließlich ist mit Phase 3 der Endausbau erreicht. Nun können die angebotenen Dienste ohne Hilfe von Drittanbietern bereitgestellt werden. Zusätzlich ist das vorhandene Personal bereits ausgebildet, so dass die Schulungskosten sinken, obwohl auf 15,5 Stellen ausgebaut wird. Damit belaufen sich die Kosten im laufenden Betrieb des Endausbaus auf ca. 2,7 – 3,0 Millionen € pro Jahr oder 7.000,- € pro Jahr für eine Kommune.

Es zeigt sich, dass ein gemeinsam betriebenes Kommunal-CERT deutlich günstiger ist, als wenn jede Kommune ihre eigene IT-Sicherheit auf dem gleichen Niveau bereitstellt. Der erhöhte Schutz rechtfertig diese Kosten, vor allem mit Blick auf Einsparungen durch verhinderte Sicherheitsvorfälle. Außerdem wird aufgrund der Häufigkeit von bestimmten IT-Sicherheitsvorfällen dieses spezielle Wissen je nach Vorfallsart bei einer Kommune nur selten, dann aber auf einen Schlag viel entsprechendes Fachpersonal benötigt. Daher ist ein zentrales Vorhalten dieses Fachwissens eine gut geeignete Möglichkeit, dieses für alle Kommunen gemeinsam sicherzustellen.

ZUSAMMENFASSUNG

Zusammenfassend lässt sich feststellen:

Besser drei Millionen pro Jahr in lokale Fachkräfte investieren und ein CERT aufbauen, als dieselbe Summe als Lösegeld an Kriminelle im Ausland bezahlen.

[5] Vgl. Konzeption für ein Kommunal-CERT für Nordrhein-Westfalen v1.02