LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

STELLUNGNAHME
17/4078

Alle Abg

Drucksache 17/13081 Stellungnahme

Prof. Dr. Jörg Schwenk

Horst Görtz Institut

Ruhr-Universität Bochum

Zusammenfassung

Aufgrund der Bedrohungslage durch Cyberkriminalität (Datendiebstahl, Ransomware) müssen die Kommunen dabei unterstützt werden, grundlegende Sicherheitsstandards einzuhalten. Daher ist der Aufbau eines Kommunal-CERT äußerst wünschenswert.

Detailfragen zur Ausgestaltung der Aufgaben des Kommunal-CERT sollten allerdings noch geklärt werden. Z.B. ist es wenig zielführend, das IT-Grundschutz-Kompendium des BSI nur zu ‚empfehlen' – dieses Kompendium ist deutlich zu umfangreich (810 Seiten in der aktuellen Ausgabe) für eine einfache Umsetzung. Hier sollte das Kommunal-CERT Lösungsvorschläge erarbeiten, die auch mit den begrenzten Mitteln einer Kommune umsetzbar sind.

Datenschutz vs. Datensicherheit

Es sollte bei den Aufgaben des Kommunal-CERT klar zwischen Datenschutz und Datensicherheit unterscheiden werden. Der (rechtlich definierte) Datenschutz ist ja bereits durch Datenschutzbeauftragte auf vielen Ebenen der öffentlichen Verwaltung präsent. Das Kommunal-CERT sollte daher möglichst ausschließlich für die (technisch definierte) Datensicherheit zuständig sein.

Bedrohungslage

Die aktuelle Bedrohungslage im Bereich der Cyberkriminalität hängt weniger von den verfügbaren Angriffsvektoren ab, als von den ‚Cybercrime-Geschäftsmodellen' die jeweils aktuell sind.

Hier ist das Beispiel Ransomware[1] zu nennen, das erst in der Kombination mit der einfachen Verfügbarkeit von Bitcoin-Zahlungssystemen zu einem Massenphänomen wurde. Ransomware ist die wohl akuteste Bedrohung für Kommunen, da das zugrundeliegende ‚Geschäftsmodell' sehr unspezifisch ist und auf jede Firma oder Organisation ‚passt', die vom Funktionieren ihrer IT abhängig ist. Da die Kosten für die Wiederherstellung von Daten (bzw. die durch den Datenverlust entstehenden Kosten) wesentlich höher sind als das geforderte ‚Lösegeld' (Ransom), eine Zahlung an den Ransomware-Erpresser aber möglicherweise weitere Straftaten gegen andere Organisationen nach sich zieht, sehe ich es als Aufgabe des Kommunal-CERT an, hier eine einheitliche Vorgehensweise zu entwickeln.

[1] https://www.zeit.de/digital/internet/2021-06/ransomware-netwalker-schadsoftware-erpressung-fbi-kriminalitaet

Beim Datendiebstahl könnte eine Untersuchung zum Wert der bei den Kommunen gespeicherten Daten sinnvoll sein. Eine Untersuchung der Firma Experian[2] gibt eine grobe Übersicht über den Wert von gestohlenen Daten im Bereich der Cyberkriminalität. Diese Liste enthält auch Daten aus dem Bereich der öffentlichen Verwaltung, z.B. Abschlusszeugnisse ($100 - $400 pro Zeugnis) und Pässe ($1000 - $2000 pro gefälschten Pass). Diese Zahlen sind die Treiber hinter den Geschäftsmodellen der Angreifer, nicht die oft beklagten ‚Schäden', die durch einen Angriff entstehen. Der Wert solcher Daten könnte auch als Indikator dienen, wie stark die einzelnen Systeme in den Kommunen abgesichert werden müssten.

Zertifizierung vs. Pentests

In der Praxis werden zwei, zueinander teilweise orthogonale, Strategien zur Absicherung gegen Cyberangriffe eingesetzt.

Zertifizierung wird in öffentlichen (Verwaltungen) und halböffentlichen (Banken, internationale Firmen) Bereichen gern eingesetzt. Sie wird durch Gesetze oder Regularien vorgeschrieben, oder ist ein internationaler de-facto-Standard. Bei der Zertifizierung im Bereich der IT-Sicherheit ist zu unterscheiden zwischen persönlichen Weiterbildungszertifikaten[3] (CISSP, CISM, ...) und der Zertifizierung der IT-Infrastruktur einer Behörde/einer Firma. Einen Überblick über die Zertifizierungsmöglichkeiten im Bereich IT-Sicherheit bietet Wikipedia[4].

Im Bereich der Zertifizierung der IT-Infrastruktur hat sich das BSI als Regulierer für Zertifizierungen in Deutschland etabliert[5], aber auch die verschiedenen TüV-Firmen sind hier stark vertreten[6]. Während den verschiedenen BSI-Zertifikaten meist klare (wenn auch teils umfangreiche) Kriterien zugrunde liegen, können Zertifizierungen nach Common Criteria[7] ziemlich vage bleiben, weil Umfang der Prüfung und die zu prüfenden Teile der IT-Infrastruktur relativ frei festgelegt werden können.

Zertifizierung kann nur eine Grundsicherheit bieten, und sollte daher nicht als einzige Strategie zur Absicherung von IT-Systemen genutzt werden. Auch ist vor überzogenen Zertifizierungsauflagen zu warnen, die in der Praxis nicht erfüllt werden können. Zertifizierung schützt nicht gegen die wechselnden Angriffsmuster der Cyberkriminalität, da sie diese nicht vorhersehen kann.

Unter **Pentesting[8]** versteht man das Ausprobieren aktueller Angriffsvektoren gegen ein laufendes IT-System in einem vom Betreiber des IT-Systems kontrollierten Prozess. Ziel ist es, potenzielle Schwachstellen *vor* einem möglichen Angreifer aus dem Bereich der Cyberkriminalität zu finden und zu beheben, um sich so gegen diese Angriffe zu schützen.

---

[2] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/
[3] https://www.digicomp.ch/blog/2020/01/05/must-have-security-zertifizierungen-2019
[4] https://en.wikipedia.org/wiki/List_of_computer_security_certifications
[5] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/zertifizierung-und-anerkennung_node.html
[6] https://www.tuvsud.com/de-de/dienstleistungen/auditierung-und-zertifizierung/cyber-security-zertifizierung
[7] https://en.wikipedia.org/wiki/Common_Criteria
[8] https://en.wikipedia.org/wiki/Penetration_test

Obwohl es standardisierte Vorgehendweisen zum Penstesting gibt (z.B. das Open Web Application Security Project OWASP[9]) liegt es im Wesen des Pentesting, keine Vorgehensweise vorzugeben, da ja auch die Vorgehensweise der Cyberkriminellen nicht beeinflusst werden kann.

Die Big-Tech-Unternehmen in den USA sind noch einen Schritt weiter gegangen und betreiben ein offenes, kontinuierliches Pentesting, das jeweils unter dem Schlagwort *Bug Bounty Programm*[10] zusammengefasst wird. Hierbei wird jeder Forscher und Techniker weltweit dazu aufgefordert, Schwachstellen in den IT-Systemen der Firmen zu finden und zu melden. Erfolgreiche Meldungen werden mit einem vorher festgelegten Geldbetrag, gestaffelt nach der Bedeutung der Schwachstelle, vergütet. Da es prestigeträchtig ist, solche Schwachstellen zu finden, werden die Namen der Forscher auch in den zugehörigen CVE-Datenbankeinträgen[11], oder auch auf den Webseiten der Unternehmen veröffentlicht.

Fazit

- Die Einrichtung eine Kommunal-CERT ist zu begrüßen, da hier Kommunen die dringend benötigte Hilfestellung zur Absicherung ihrer Systeme bekommen können.
- Das Kommunal-CERT sollte sich auf die Datensicherheit konzentrieren, da der Datenschutz organisatorisch schon auf allen Ebenen der Verwaltung verankert ist.
- Durch Beobachtung der Trends der Cyberkriminalität (z.B. Ransomware) kann das Kommunal-CERT klare Handlungsanweisungen zur Vermeidung von Angriffen geben. Es kann auch eine Koordinierungsrolle bei ethisch schwierigen Entscheidungen übernehmen (z.B. ob Ransom gezahlt wird oder nicht).
- Die Bedrohungslage der Kommunen ist noch unklar. Es gibt noch keine systematischen Untersuchungen darüber, welche kommunal vorgehaltenen Daten für Angreifer einen vermarktbaren Wert darstellen.
- Eine umfangreiche Zertifizierung der IT ist für einzelne Kommunen nicht zu leisten, diese kann nur für größere kommunale Rechenzentren in Frage kommen.
- Ein vom Kommunal-CERT koordiniertes Pentesting-Programm kann die Sicherheit der kommunalen IT gegenüber Cyberangriffen wesentlich verbessern.

[9] https://en.wikipedia.org/wiki/OWASP
[10] https://en.wikipedia.org/wiki/Bug_bounty_program
[11] https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures