Ein starker Hebel für mehr IT-Sicherheit

Ob ideologisch oder finanziell getrieben, deutsche Kommunen sehen sich immer öfter komplexen Cyber-Angriffen gegenüber, denen sie kaum etwas entgegenzusetzen haben. Um mehr Sicherheit herzustellen, wird in Nordrhein-Westfalen die interkommunale Zusammenarbeit weiter gestärkt.

Wer ein Gefühl dafür bekommen möchte, in welchen Dimensionen Cybercrime heute stattfindet, muss nur wenige Monate zurückblicken. Mitte Juli waren Strafverfolgungsbehörden aus Deutschland, Frankreich, Italien, den Niederlanden, Schweden, Spanien, der Schweiz und den USA – unterstützt durch Europol und Eurojust sowie unter Beteiligung weiterer europäischer Länder – gegen das prorussische Hacktivisten-Kollektiv NoName057(16) vorgegangen. Im Rahmen der international koordinierten Maßnahmen wurde ein Botnetz abgeschaltet, das sich aus mehreren Hundert global verteilten Servern zusammensetzte und für Distributed-Denial-of-Service-Attacken (DDoS) eingesetzt wurde. Zudem wurden in Deutschland sechs Haftbefehle gegen Beschuldigte erwirkt, ein weiterer Haftbefehl wurde durch die spanischen Behörden erlassen. Nach allen Beschuldigten wird international und teils öffentlich gefahndet.

Es geht um eine ganze Menge: Die Unversehrtheit unserer westlichen Demokratie steht auf dem Spiel. Denn No-

Kompakt

- Cyber-Kriminelle mit verschiedenen Motiven, finanziell und personell bestens ausgestattet, treffen auf Kommunen und ihre fragmentierte IT, die sich schwertun, Angriffen etwas entgegenzusetzen.
- Mehr Zusammenarbeit und eine Konsolidierung bei Soft- und Hardware würden für deutlich mehr Sicherheit sorgen. In Nordrhein-Westfalen wird bereits daran gearbeitet.
- Ziel ist eine kluge Kombination von dezentralen und zentralen Bestandteilen einer IT-Sicherheitsarchitektur für die Kommunen in NRW.

Verfasst von

Kerstin Pliquett
Die Autorin ist Geschäftsleiterin des KDN – Dachverband kommunaler IT-Dienstleister. Zuvor war sie unter anderem bei der Südwestfalen-IT tätig.

Michael Schwengers
Der Autor arbeitet in der Öffentlichkeitsarbeit des KDN. Davor hat er unter anderem für das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) kommuniziert.

Name057(16) ist ganz offensichtlich auf einer ideologisch motivierten Mission. Auf der Cybercrime-Bildfläche erschienen ist die Gruppe im März 2022, also unmittelbar nach Beginn des russischen Angriffskriegs auf die Ukraine. Seitdem stellt sie mit DDoSia eine Plattform bereit, über die sich Unterstützerinnen und Unterstützer mit ihren eigenen Ressourcen leicht an DDoS-Angriffen beteiligen können. Eine detaillierte Analyse der Aktivitäten von NoName057(16) hat die Insikt Group vorgelegt. Laut der Forschungsorganisation, die zum amerikanischen IT-Sicherheitsunternehmen Recorded Future gehört, wurden im Zeitraum von Juni 2024 bis Juli 2025 über DDoSia 3.776 einzelne Ziele angegriffen. Über 40 Prozent der Attacken galten Regierungsorganisationen beziehungsweise der öffentlichen Verwaltung.

Das Beispiel mag in seiner Größenordnung zwar nicht die Regel sein, zeigt allerdings ziemlich typisch die Gefahren für die IT-Sicherheit in Deutschlands Kommunen auf: Ideologisch motivierte Hackergruppen, die weltweit organisiert sind, dezidierte Kenntnisse aus allen relevanten Bereichen zusammenführen und mit reichlich finanziellen sowie personellen Ressourcen ausgestattet sind, führen Advanced Persistent Threats (APT) gegen Städte, Gemeinden und Kreise aus. Als APTs werden Cyber-Angriffe verstanden, die besonders komplex, andauernd und zielgerichtet sind. In seinem Bericht „Die Lage der IT-Sicherheit in Deutschland 2024“ geht das Bundesamt für Sicherheit in der Informationstechnik (BSI) davon aus, dass in der Bundesrepublik derzeit 22 solcher ATP-Gruppen aktiv sind. Die Kommunen sind den Kriminellen in Bezug auf ihre IT-Sicherheit dramatisch unterlegen, da sie schon meist kaum wissen, wie sie ihre eigentlichen Aufgaben erfüllen sollen, und froh sind, die Verwaltungsdigitalisierung ordentlich hinzubekommen.

Nicht nur Großstädte geraten ins Visier

Zu den ideologisch motivierten Angreifenden gesellen sich cyberkriminelle Gruppen, die sich ausschließlich dafür interessieren, mithilfe ihrer Ransomware Geld von Organisationen oder Einzelpersonen zu erpressen. Im Zeitraum vom 1. Juni 2022 bis zum 30. Juni 2023 haben solche Ransomware-Gruppen insgesamt 27 kommunale Einrichtungen in Deutschland attackiert – von der ländlichen Gemeinde mit 2.800 Einwohnenden bis zur Großstadt, in der 1,8 Millionen Menschen leben. Das geht aus dem BSI-Bericht „Die Lage der IT-Sicherheit in Deutschland 2023“ hervor.

Ein besonders heftiger Ransomware-Angriff fand in der Nacht zum 30. Oktober 2023 auf eines unserer Mitglieder statt. Eine Gruppe mit dem Namen Akira hatte sich über eine VPN-Verbindung Zugang zu den Servern des kommunalen IT-Dienstleisters Südwestfalen-IT verschafft und dort gespeicherte Daten verschlüsselt. In der Folge fielen mehr als 22.000 Arbeitsplätze und rund 160 Fachverfahren der 72 Mitglieder des Zweckverbands aus – mit erheblichen Konsequenzen für die 1,6 Millionen Bürgerinnen und Bürger in den betroffenen Kommunen. Die vollständige Wiederherstellung aller Systeme nahm elf Monate in Anspruch und verursachte Kosten von circa 2,8 Millionen Euro.

Die Südwestfalen-IT hat die aus dem Vorfall gewonnenen Erkenntnisse genutzt, um die eigene Resilienz gegen Cyber-Attacken mithilfe von technischen, prozessualen und organisatorischen Maßnahmen weiter zu erhöhen. Noch mehr Widerstandfähigkeit lässt sich nach Ansicht von Mirco Pinske erreichen, der seit dem 1. Februar 2024 Geschäftsführer bei Südwestfalen-IT ist, wenn die eingesetzten Technologien konsolidiert werden: „Die Vielfalt der Anwendungen muss reduziert werden, für gleichartige Aufgaben darf es im Verbandsgebiet auch nur jeweils ein System geben. Das reduziert nicht nur den

Aufwand für Wartung und Weiterentwicklung. Vor allem bieten wir Kriminellen dadurch weniger Angriffsfläche."

Nach unserer Auffassung ist genau das die richtige Stoßrichtung: Wenn wir als Kommunen und kommunale IT-Dienstleister der immensen Schlagkraft von ideologisch oder finanziell motivierten Cyber-Kriminellen etwas entgegensetzen wollen, müssen wir unsere Kräfte konzentrieren. Denn allein verfügt keine Kommune über das erforderliche Know-how, das erforderliche Personal und die erforderlichen Finanzen, um ihre digitale Infrastruktur wirksam zu schützen – keine Großstadt und erst recht keine kleine Gemeinde. Ähnlich gilt das für die kommunalen IT-Dienstleister. Arbeiten aber alle eng zusammen, lässt sich ein ziemlich performantes IT-Sicherheitsregime etablieren.

Konkret bedeutet das, kommunenübergreifend die Anzahl der zu schützenden Software und Hardware und damit auch die Anzahl der potenziellen Angriffsflächen zu minimieren. Wenn die 427 Städte, Gemeinden und Kreise in Nordrhein-Westfalen (NRW) beispielsweise nicht zehn verschiedene Anwendungen für ein und dasselbe Fachverfahren einsetzen würden, sondern nur zwei, dann hätte das für die Sicherheit einen erheblichen Effekt. Und wenn diese zwei Anwendungen nicht als On-Premises-Instanzen auf Servern in den Kommunen vor Ort laufen, sondern als Software-as-a-Service (SaaS) über eine Cloud bereitgestellt werden, nimmt auch die Anzahl an Installationen ab und die Sicherheit steigt weiter.

Bei der Hardware lohnt sich eine Konsolidierung ebenfalls – tatsächlich noch mehr als bei der Software. Denn vor allem in kleineren Gemeinden kommen oft Server und Speicherlösungen zum Einsatz, die nicht ausreichend geschützt werden, weder vor Cyber-Attacken noch vor Bränden, Hochwasser oder sonstigen Katastrophen. Software und Daten in einem zentralen Rechenzentrum vorzuhalten und eine geschützte Kommunikation für den Austausch zu nutzen, bietet da in der Regel mehr Sicherheit. Natürlich passiert das zum Teil schon heute. Die KDN-Mitglieder betreiben bereits seit Jahren und Jahrzehnten für die Kommunen in NRW Rechenzentren in verschiedenen Größen. Viele Städte und Gemeinden nutzen aber außerdem nach wie vor zumindest zum Teil ihre eigene Infrastruktur. Eine weitere Konzentration der kommunalen Rechenzentren auf wenige sehr performante und sehr gut geschützte Standorte, ein noch intensiverer Einsatz von standardisierten VPN-Lösungen und gemanagten Firewalls sowie eine stärkere Netz-Segmentierung würde das IT-Security-Niveau weiter anheben.

Damit eine solche IT-Konsolidierung gelingt, ist eine zielführende Koordination der Kooperation erforderlich: Zum einen müssen die spezifischen Sicherheitsanforderungen und darüber hinausgehenden Interessen der einzelnen Akteure aufgenommen und in Einklang gebracht werden – auch mit Blick auf künftige Technologien. Zum anderen kommt es darauf an, die vorhandenen Kompetenzen und Best Practices zu sammeln und zusammenzuführen. In NRW arbeiten wir gemeinsam mit den kommunalen IT-Dienstleistern und den Kommunen daran, die bestehende Kooperation stetig auszubauen und kontinuierlich zu verbessern.

Weitere wertvolle Beiträge der Kooperation

Durch diese Zusammenarbeit werden einige Vorteile realisiert:

- Es entsteht ein gemeinsames Bewusstsein für IT-Security, was sich auch positiv auf die Awareness auswirkt.

Handlungsempfehlungen

1. **Softwarelandschaft prüfen:** Welche Anwendungen sind überhaupt vorhanden und welche werden tatsächlich genutzt? Sind alle Lizenzen aktuell oder werden Anwendungen eventuell nicht mehr unterstützt? Gibt es Eigenentwicklungen und wenn ja, wie werden sie abgesichert?
2. **Hardwarelandschaft prüfen:** Welche Server und Speicherlösungen werden vor Ort betrieben und weshalb sind sie erforderlich? Wer kümmert sich um die Sicherheit der Hardware vor Ort und welche Maßnahmen werden derzeit ergriffen? Lassen sich Anwendungen und Daten in ein kommunales Rechenzentrum verlagern?
3. **Mitarbeitende schulen:** Sind die Beschäftigten mit den relevanten Sicherheitsmaßnahmen vertraut? Wie regelmäßig erfolgen Schulungen?
4. **Business Continuity etablieren:** Gibt es Pläne dafür, was bei einem IT-Sicherheitsvorfall passiert? Wie können die wesentlichen Aufgaben weiterhin erfüllt werden und wie lässt sich die IT wiederherstellen?
5. **Sicherheitskonzept erstellen:** Ist ein Konzept vorhanden, in dem alle Sicherheitsrisiken aufgeführt und bewertet sind und in dem die Sicherheitsmaßnahmen aufgeführt werden?

- Es entsteht eine gemeinsame Governance, die den Einsatz von Software und Hardware über alle Ebenen hinweg regelt und sichere Prozesse definiert. Dadurch lassen sich die einzelnen Sicherheitsmaßnahmen leichter ausrollen und bei einem IT-Security-Vorfall kann schneller reagiert werden.

Daher sprechen wir uns für eine kluge Kombination von dezentralen und zentralen Bestandteilen einer IT-Sicherheitsarchitektur für die Kommunen in NRW aus. Wie viele unterschiedliche Anwendungen dann am Ende für ein Fachverfahren zur Verfügung stehen und wie viele Rechenzentren wo, von wem und mit welchen Leistungen betrieben werden – das wird sich in der Umsetzung herausstellen. Wichtig ist heute, dass wir den in NRW eingeschlagenen Weg konsequent weitergehen. Dass ein solcher Weg zum Erfolg führt, haben übrigens die Sparkassen vorgemacht. Sie haben schon vor rund 20 Jahren damit begonnen, ihre IT zu konsolidieren und die vielen kommunalen Organisationen in eine zentrale IT-Organisation zu verlagern. Das ging nicht von heute auf morgen und sicher auch nicht immer vollständig reibungslos. Jetzt sind sie aber für sämtliche Herausforderungen unserer digitalen Welt hervorragend aufgestellt. ■

„Wenn wir als Kommunen und kommunale IT-Dienstleister der immensen Schlagkraft von ideologisch oder finanziell motivierten Cyber-Kriminellen etwas entgegensetzen wollen, müssen wir unsere Kräfte konzentrieren.“

- Es entsteht ein umfassendes Schulungsangebot zu allen Aspekten der IT-Sicherheit, das die verschiedenen Partner im Verbund organisieren.
- Es entsteht ein Business Continuity Management, das in den einzelnen Kommunen ansetzt und aus der übergreifenden Perspektive konzipiert ist.

Gegen all das lässt sich einwenden, dass eine zusammengeführte IT ein besonders attraktives Ziel für Hackergruppen ist – schließlich wären hier die Folgen einer erfolgreichen Attacke immens. Hinzu kommt, dass auch die Cyber-Kriminellen ihre Anstrengungen konzentrieren und sich auf die verbleibenden Technologien und Ziele konzentrieren können. Besser wäre es deshalb aus Sicht von Konsolidierungskritikerinnen und -kritikern, weiterhin als kleine Einheit unter dem Radar der Hacktivistinnen sowie Hacktivisten zu bleiben und nicht angegriffen zu werden. Theoretisch sind die Überlegungen zwar nachvollziehbar, praktisch ergeben sie aus unserer Sicht aber wenig Sinn. Denn ein Blick auf die Attacken der zurückliegenden Monate und Jahre zeigt deutlich, dass eben nicht nur besonders große Einrichtungen das Ziel von Angriffen waren, sondern Kommunen jeder Größe. Und angesichts der hohen Zahl an Attacken ist es im Grunde nur eine Frage der Zeit, bis es einen selbst erwischt.