Cybersicherheit

Angriffserkennung in der kommunalen Verwaltung

Interview mit Thomas Stasch, CISO & Centerleiter Competence Center Security (KomCERT) bei der regio iT gesellschaft für informationstechnologie mbh.

In den letzten Monaten gab es immer wieder Meldungen zu Hackerangriffen auf Kommunen. Thomas Stasch, Chief Information Security Officer und Leiter des KomCERTs des IT-Dienstleisters regio iT, stand uns für Fragen rund um das Thema Cybersicherheit für kommunale Verwaltungen zur Verfügung. Wie können sich Kommunen am besten gegen Hackerangriffe schützen? Was sind typische Anzeichen für einen Hackerangriff? Und was ist zu tun, wenn ein Hackerangriff auffällt? Zu diesen und weiteren Fragen hält Thomas Stasch zahlreiche Antworten für Kommunen bereit.

Wie können sich Kommunen am besten gegen Hackerangriffe schützen?

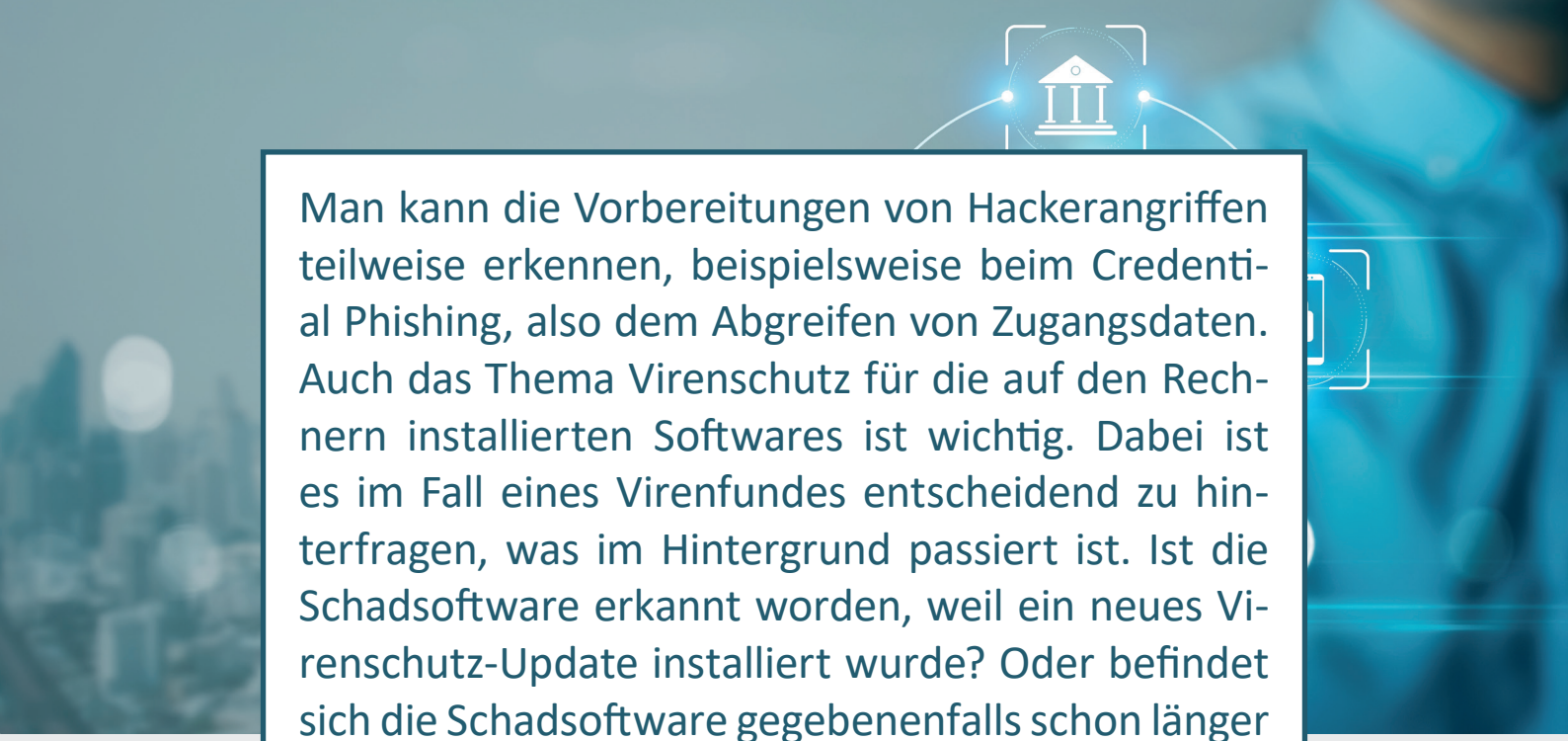
»Kommunen können sich nur durch ein solides Informationssicherheitsmanagementsystem (ISMS)

KDN

schützen, das organisatorische Regelungen (insbesondere in Bezug auf die technischen Umsetzungen) beinhaltet. Angefangen von einem adäquaten Virenschutz bis zur Schulung und Sensibilisierung aller Mitarbeitenden. Es ist heutzutage Pflicht, Mitarbeitende darin zu unterweisen, eine Phishing-Mail zu erkennen, wenn eine solche vorliegt. Das sind Vorkehrungsmaßnahmen, die man unbedingt vornehmen muss. Andernfalls riskiert man, dass es früher oder später zu einem Sicherheitsvorfall kommt. Auf der Übersichtskarte Kommunaler Notbetrieb, betrieben von Jens Lange, dem IT-Sicherheitsbeauftragten der Stadt Kassel, sind alle in Deutschland bekannt gewordenen Fälle aufgelistet. Ich verfolge diese Seite mit sehr viel Neugier, auch wenn die dort erfassten Fälle aus meiner Sicht nur die Spitze des Eisbergs darstellen. Ich denke, dass es aktuell nur rund zehn Prozent aller Fälle in die Presse schaffen. Wenn ich das hochrechne, müsste es folglich in Deutschland schon jede achte bis zehnte Kommune einmal getroffen haben. Daher ist klar: Jede Kommune sollte sich intensiv mit dem Thema IT-Sicherheit befassen. Sie sollte einen Verantwortlichen dafür bestellt haben, der möglichst nicht in der IT arbeitet, sondern direkt an den Hauptverwaltungsbeamten berichtet.«

Was sind Anzeichen für einen Hackerangriff?

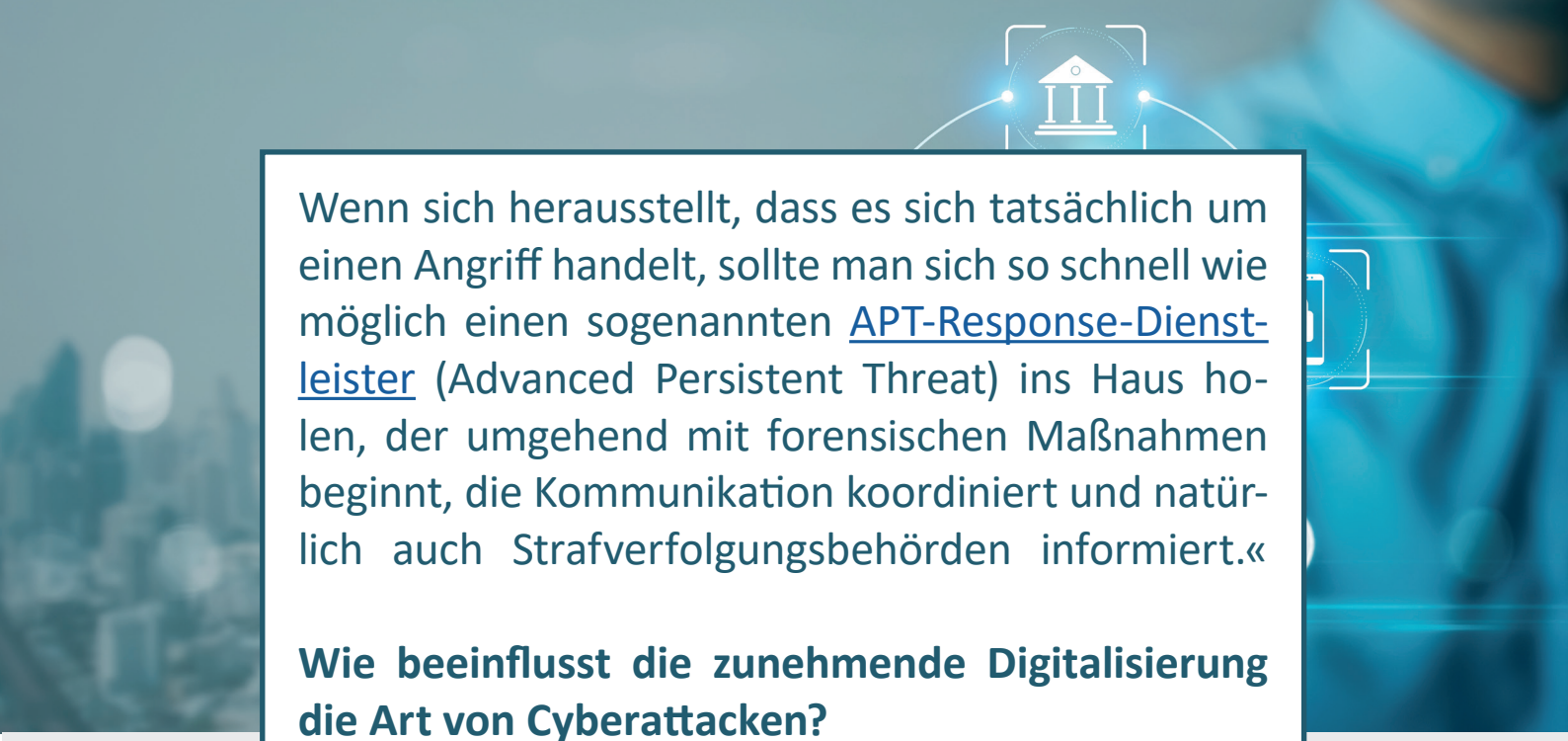
»Professionelle Hackerangriffe werden meist erst dann erkannt, wenn Systeme verschlüsselt wurden oder Daten abgeflossen sind. Deswegen sollte man unterschiedliche Erkennungsmechanismen nutzen.



Man kann die Vorbereitungen von Hackerangriffen teilweise erkennen, beispielsweise beim Credential Phishing, also dem Abgreifen von Zugangsdaten. Auch das Thema Virenschutz für die auf den Rechnern installierten Softwares ist wichtig. Dabei ist es im Fall eines Virenfundes entscheidend zu hinterfragen, was im Hintergrund passiert ist. Ist die Schadsoftware erkannt worden, weil ein neues Virenschutz-Update installiert wurde? Oder befindet sich die Schadsoftware gegebenenfalls schon länger im System und hat entsprechend mehr Unheil angerichtet? Das sind Fragen, die ich mir als verantwortlicher Experte ebenfalls stellen muss. Und davon sind Verwaltungen in Deutschland aus meiner Sicht noch weit entfernt, weil nur große Kommunen über Angestellte verfügen, die sich hauptamtlich mit dem Thema Operative Cyber Security beschäftigen und die diese Fragen stellen und beantworten können.«

Was sollten Kommunen im Falle eines Hackerangriffs als Erstes tun?

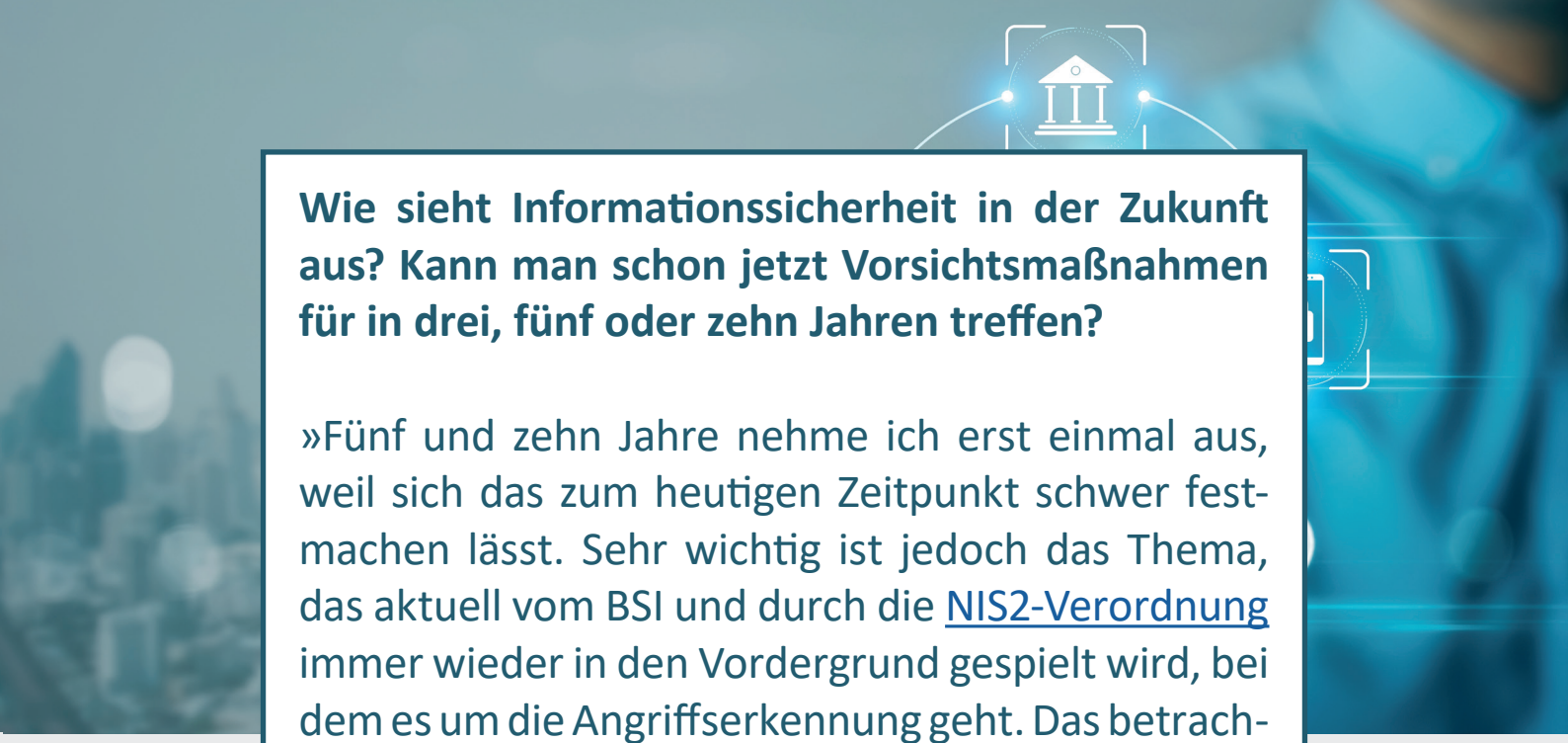
»Der erste Schritt ist auf jeden Fall jemanden einzubinden, der über entsprechendes Wissen und über Erfahrung verfügt und den Angriffsfall sofort meldet. Kommunen in NRW können sich an das CERT des Landes NRW wenden. Kommunen, die ein eigenes CERT beauftragt haben, wie unsere Kunden, wenden sich an unser KomCERT, das bei einem sicherheitsrelevanten Vorfall alle notwendigen Maßnahmen umgehend einleitet. Beim Bundesamt für Sicherheit und Informationstechnik (BSI) können sich betroffene Kommunen ebenfalls Hilfe holen.



Wenn sich herausstellt, dass es sich tatsächlich um einen Angriff handelt, sollte man sich so schnell wie möglich einen sogenannten APT-Response-Dienstleister (Advanced Persistent Threat) ins Haus holen, der umgehend mit forensischen Maßnahmen beginnt, die Kommunikation koordiniert und natürlich auch Strafverfolgungsbehörden informiert.«

Wie beeinflusst die zunehmende Digitalisierung die Art von Cyberattacken?

»Die Digitalisierung hat einen direkten Einfluss auf die Art der Cyberattacken. Wir stellen fest, dass die Angriffsvektoren ständig im Wandel sind und nicht mehr ausschließlich durch Phishing-E-Mails ausgelöst werden. Angreifende nutzen nun auch andere Schwachstellen in Systemen aus, was die Bedrohungslage erheblich verändert. Mit zunehmender Digitalisierung steigt auch das potenzielle Schadensausmaß eines Angriffs. In der heutigen Zeit können betroffene Kommunen nahezu handlungsunfähig werden. Zudem eröffnet die kontinuierliche Bereitstellung neuer Zugänge für Bürgerinnen und Bürger zusätzliche Angriffsmöglichkeiten. Dies führt zu einer Zunahme des Risikos sowie zu einem erhöhten Schadenpotenzial für die betroffenen Kommunen. Angesichts dieser Entwicklungen wird deutlich, wie wichtig es ist, Risikomanagement im Umgang mit Cyberangriffen zu betreiben – Stichwort „Incident Readiness“. Jede Kommune sollte sich dieser Thematik bewusst sein und entsprechende Maßnahmen ergreifen, um ihre Systeme und Daten zu schützen.«



Wie sieht Informationssicherheit in der Zukunft aus? Kann man schon jetzt Vorsichtsmaßnahmen für in drei, fünf oder zehn Jahren treffen?

»Fünf und zehn Jahre nehme ich erst einmal aus, weil sich das zum heutigen Zeitpunkt schwer festmachen lässt. Sehr wichtig ist jedoch das Thema, das aktuell vom BSI und durch die NIS2-Verordnung immer wieder in den Vordergrund gespielt wird, bei dem es um die Angriffserkennung geht. Das betrachten viele Kommunen heute noch als Randthema und hoffen, dass ein gewisser Schutz und eine Firewall ausreichen – aber das ist nicht der Fall. Wir reden hier von topaktuellen Technologien und Detektionssystemen, auf die man zugreifen und die man beherrschen muss. Dass das Thema an Fahrt gewinnt, sieht man auch daran, dass die Erkennungs- und Reaktionsmechanismen inzwischen auch für kritische Unternehmen verpflichtend sind. Ich erwarte, dass die Kommunen früher oder später als kritisch eingestuft werden. Und das finde ich auch richtig, weil die Daten, die dort verarbeitet werden, für den Staat sehr wichtig sind. Verwaltungen verantworten das virtuelle Abbild von allen Bürgerinnen und Bürgern. Ich zitiere hier gerne Dirk Schumacher, Leiter Stabsstelle IT-Sicherheit und IT-Strategie im Personal- und Organisationsamt der Bundesstadt Bonn, der einmal gesagt hat: *Wenn es dir bei einer Kommune gelingt, dich sterben zu lassen, dann wird es sehr schwer nachzuweisen, dass du noch lebst.*«