Spotlight: Cybersecurity in der öffentlichen Verwaltung

Informationstechnologie heute:
digital, innovativ, kognitiv, sicher

IBM

Cybersecurity in der öffentlichen Verwaltung

Im Sommer 2018 hat die Bundesregierung die Gründung einer Agentur für Cybersicherheit bekannt gegeben. Ziel der neuen Institution soll es sein, den Staat und seine Bürger in Zukunft besser vor Hackerangriffen zu schützen. Der Ehrgeiz ist es, mindestens „so schnell zu sein, wie die Angreifer und Täter“ (Ursula von der Leyen). Denn immer öfter richten Cyberkriminelle ihre Attacken auf die Sicherheit des Landes, der Behörden, der Wirtschaft und der privaten Anwender. Die „Agentur für Innovation in der Cybersicherheit“ wird ihre Arbeit voraussichtlich 2019 aufnehmen.

Die Gründung ist ein klares Signal: Cybersicherheit ist Voraussetzung für eine erfolgreiche Digitalisierung. Gerade für Behörden ist das Thema heute eine sehr ernste Herausforderung. Immer häufiger geraten sie ins Visier der Cyberangreifer. Das Schadenspotenzial hat heute erschreckende Ausmaße angenommen. So hat das Bundesamt für Informationstechnik (BSI) in den zurückliegenden Jahren immer öfter Angriffe auf Energie-, Wasser- und Nahrungsversorger registriert. Man kann sich leicht ausmalen, welches kriminelle Potential erfolgreiche Angriffe auf diesen Sektor annehmen könnten. Organisierte Erpressungen im großen Stil wären möglich – James Bond lässt grüßen. Wie nahe die Szenarien liegen, zeigt das prominenteste Opfer einer Cyberattacke – der deutsche Bundestag. Wie im März 2018 bekannt wurde, gelang es einer Hackergruppe – man vermutet eine namens „Snake“ dahinter – in das Netzwerk des Bundestags einzudringen und Daten zu stehlen. Das wahre Ausmaß des Schadens ist nicht bekannt.

Mit der neuen Agentur für Cybersicherheit will man in Zukunft solchen Angriffen auf deutsche Behörden zuvorkommen. Die Spezialisten sollen dabei auch aussichtsreiche Forschungsarbeiten zum Thema Security identifizieren, fördern und zum Schutz der Behörden nutzbar machen. Das Signal ist wichtig und richtig, die Gründung der Agentur für Cybersicherheit ist ein wichtiger Schritt, um Vertrauen aufzubauen. Es wird aber die Behörden nicht von ihrer Pflicht entbinden, selbst aktiv zu werden, um den Bürgern und Unternehmen im Zeitalter der digitalen Transformation sichere, interaktive Daten- und Kommunikationsprozesse mit ihr zu gewährleisten. Dazu zwingt sie alleine schon die neue Datenschutzgrundverordnung. Denn auch Behörden unterliegen bei der Verarbeitung personenbezogener Daten den DSGVO-Vorschriften. Auch sie müssen sicherstellen, dass angemessene technische und organisatorische Maßnahmen zur Sicherung personenbezogener Daten getroffen wurden.

Ein Partner für diese Aufgabe ist IBM – das Unternehmen unterstützt Behörden weltweit dabei, den Bürgern die benötigten Dienstleistungen anzubieten und sie zu schützen. Das breite Portfolio an Sicherheitslösungen stützt sich dabei auf einmalige und langjährige Erfahrungen mit Digitalisierungs- und Sicherheitsprojekten auf der ganzen Welt. Das Angebot umfasst zum Beispiel Unterstützung beim IT-Service-Management, IT-Service- und Risiko-Management mit IBM Analytics und IBM Watson® oder IBM Watson® for Cybersecurity. Auch die neue Blockchain-Technologie – bei deren Erschließung IBM zu den Vorreitern zählt – bietet hier Möglichkeiten zur Verbesserung der Sicherheit.

Service-Management kombiniert mit Analytics ermöglicht einheitliches IT-Lagebild

Um zu wissen, wo Gefahren drohen, ist es wichtig, die Gesamtlage der IT-Infrastruktur im Blick zu behalten. Die richtige Disziplin hierfür ist das IT-Service Management, denn es ermöglicht die Erstellung eines einheitlichen IT-Lagebilds – auch über unterschiedliche Sicherheitsdomänen hinweg.

IT-Service Management (ITSM) kann einen wichtigen Beitrag zur Cybersecurity in Behörden leisten. Service Management umfasst alle Bemühungen, den Fokus der IT-Verantwortlichen von der technischen Sicht auf Betriebsstrukturen und Produkte auf ein höheres Maß an Serviceleistung und damit Kundenorientierung zu verlagern. Das IT-Service Management wird auch in den Behörden meist für die VS-NfD („Verschlusssache – nur für den Dienstgebrauch“) - Domänen einheitlich angewandt. Das Problem besteht darin, dass Domänen mit höherer Sicherheitseinstufung in einer autarken Infrastruktur aufgehoben und vom IT-Service Management daher ausgenommen sind, was wiederum auf Kosten eines einheitlichen Gesamtbildes geht. Das kann durch die Darstellung in einem übergreifenden IT-Lagebild gewährleistet werden, welches sämtliche Sicherheitsdomänen umfasst. IBM Software hilft, das zu erreichen.

Die Bereitstellung der IT-Services wird in der Sicherheitsdomäne VS-NfD gesteuert. Die dafür benötigten Konfigurationsdaten, Statusinformationen (Events) oder Störungsmeldungen der Anwender mit Einstufung VS-NfD oder geringer werden in das IT-Service Management Environment (ITSME) übertragen. Das für die Zulassung zuständige, regelbasierte Security Gateway, sorgt für den sicheren Netzübergang und verhindert gleichzeitig den ungewollten Abfluss von Daten höherer Einstufung in die Sicherheitsdomäne VS-NfD. Zudem ermöglicht das Gateway den Rückfluss relevanter Daten zur Aktualisierung und Steuerung von Aktivitäten in der Sicherheitsdomäne „High“. Daraus folgt, dass ein einheitliches IT-Service-Management über Sicherheitsdomänen-Grenzen hinweg machbar ist.

Ein Großteil der Aufgaben zur Bereitstellung der IT-Services kann schon aus der Sicherheitsdomäne VS-NfD erfolgen. IBM hat das IT-Service Management Environment (ITSME) beispielsweise im IT-SysBw mit IBM Software realisiert – auf der gleichen Basis, auf der auch die BWI-Anteile administriert werden. Durch BSI-zertifizierte Partner kann diese Lösung auch auf Domänen unterschiedlicher Sicherheitseinstufungen erweitert werden.

Ein noch umfassenderes Gesamtbild ergibt sich durch die Einbindung von intelligenten Programmen und Methoden in Verwaltungsprozesse. Kombinierte Risikomanagement-Funktionen der IBM Software-Familie lassen sich beispielsweise um die IBM Service-Management-Funktionen ergänzen. Das Lagebild wird dadurch vollständiger. Und mit der Unterstützung von IBM Analytics und IBM Watson® lassen sich Gefahrenlagen zudem detailliert erfassen und Lagebilder mit unterschiedlichsten Informationen, wie beispielsweise Texten, Audiodateien und Geoinformationen korrelieren. Es entsteht ein umfassendes Bild, das die Gefahren auf den unterschiedlichen Ebenen der Domänen sichtbar macht.

Blockchain bietet neue Möglichkeiten für mehr Sicherheit in der Verwaltung

Die Vorstellung einer zentralen Datenbank, die man nicht manipulieren oder zensieren kann, ist gerade für die öffentliche Verwaltung verlockend. Die Blockchain-Technologie erlaubt diese Möglichkeit – und bietet zudem den Reiz, öffentliche Daten frei zugänglich zu machen, private aber gleichzeitig zu schützen. Das eröffnet viele neue Chancen für mehr Sicherheit in der Verwaltung.

Viel wurde in letzter Zeit über Blockchain geschrieben. Als neue Technologie zur Verbesserung von Datenschutz und -sicherheit in Behörden trat sie bislang noch nicht in Erscheinung. Dabei ist das Potential gerade für die öffentliche Verwaltung groß. Denn die Blockchain-Technologie ermöglicht es, geschäftliche Sachverhalte in einer logischen, zentralen Datenhaltung abzulegen – also Vorgänge wie Aktienkauf, eine Heirat, ein Handelsregistereintrag oder auch die Beschaffung oder Wartung eines Kampfjets. Die Besonderheit: Die Datenbank ist physisch hochgradig verteilt – und gerade dadurch besonders vor Manipulationen geschützt.

IBM hat Blockchain im Rahmen einer Open-Source-Initiative weiterentwickelt und Kinderkrankheiten wie Skalierung, Performance und effizienter Betrieb gelöst. Dadurch ist es jetzt prinzipiell möglich, beliebige Sachverhalte in einem Netzwerk zwischen verschiedenen Beteiligten abzuspeichern. Kritische Eigenschaften wie Sicherheit, Unveränderbarkeit, Nachvollziehbarkeit oder Protokollierung sind in Blockchain bereits eingebaut. Damit bietet Blockchain gerade für öffentliche Verwaltungen eine ideale Basis, um zentrale Informationsbestände aufzubauen – und das konsistent und ohne besonderen Integrationsaufwand.

Beispiele für Einsatzfelder in der Öffentlichen Verwaltung sind:

- Alle Arten von Registern.
- Alle Fachverfahren, bei denen Informationen dezentral entstehen und verarbeitet werden und trotzdem zentrale Ansichten benötigt werden.
- Alle Bereiche, in denen Betrug durch asymmetrische Informationsbestände an der Tagesordnung steht (Mehrwertsteuer-Karussell etc.).

IBM ist eine treibende Kraft bei der Weiterentwicklung von Blockchain und verfolgt dabei weiterhin den Open-Source-Ansatz. Gleichzeitig bietet das Unternehmen Beratung zum Einsatz von Blockchain, unterstützt bei ersten Schritten mit der Blockchain-Garage im Labor Böblingen und stellt Kunden die notwendige Infrastruktur in bewährter IBM Qualität bereit – sei es im Rechenzentrum des Kunden oder auch mit der IBM Cloud™ in hybriden Cloud-Umgebungen.

Cyberangriffe schnell einschätzen und bewerten – mit Hilfe von KI

Auch die Künstliche Intelligenz (KI) lässt sich zur Erhöhung der IT-Sicherheit nutzen. Ein Paradebeispiel dafür ist IBM Watson® for Cybersecurity – die Technologie revolutioniert die Arbeit der Security-Analysten.

IBM Watson® ist ein nach dem IBM Gründer Thomas J. Watson benanntes System, das KI mit anspruchsvoller analytischer Software kombiniert. Die Spezialität des Systems ist die Beantwortung von Fragen in natürlicher Sprache auf Basis massiver, auch unstrukturierter Daten. Die Fähigkeit macht IBM Watson® gerade auch für die Cybersecurity-Analysten besonders interessant, beantwortet es doch die Fragen von Analysten auf Basis hunderter interner und externer Datenquellen - eine immense Hilfe, um potentielle Angriffe schnell zu erkennen.

Das Informations- und Datenmaterial, aus dem IBM Watson® schöpft, umfasst eine riesige Menge an Informationen aus Tausenden von Blogs, Artikeln in Zeitschriften für Cybersicherheit, Nachrichten, Forschungsarbeiten und mehr.

Die meisten Computer können auf diese unstrukturierten Inhalte nicht automatisch zugreifen, so dass Sicherheitsanalysten Stunden damit verbringen müssten, Online-Inhalte manuell durchzusuchen.

Das aber leistet IBM Watson® für sie. Mit der Watson-Technologie werden die Fähigkeiten einer Störmeldung (Security Incident) um die des Event Managements erweitert.

In Ergänzung zur Echtzeitanalyse wertet Watson Kontext- und historische Daten aus und erkennt und visualisiert Zusammenhänge. Damit können Angriffe effizienter identifiziert und aufgeklärt werden.

Behörden können so Angreifern den entscheidenden Schritt voraus sein.

Aufbau der IT-Sicherheit und Nutzung von Synergien notwendig

Die zunehmende Vernetzung industrieller Infrastrukturen im Zuge des Internet of Things bzw. der Industrie 4.0 erfordert neuartige Schutzmaßnahmen für heutige IT-Umgebungen auch in Behörden und Verwaltungen. Dazu zählen auch organisatorische Maßnahmen wie beispielsweise die Etablierung eines übergreifenden Cyber Security Operation Center (CSOC) wie das des Bundesverteidigungsministeriums (BMVg).

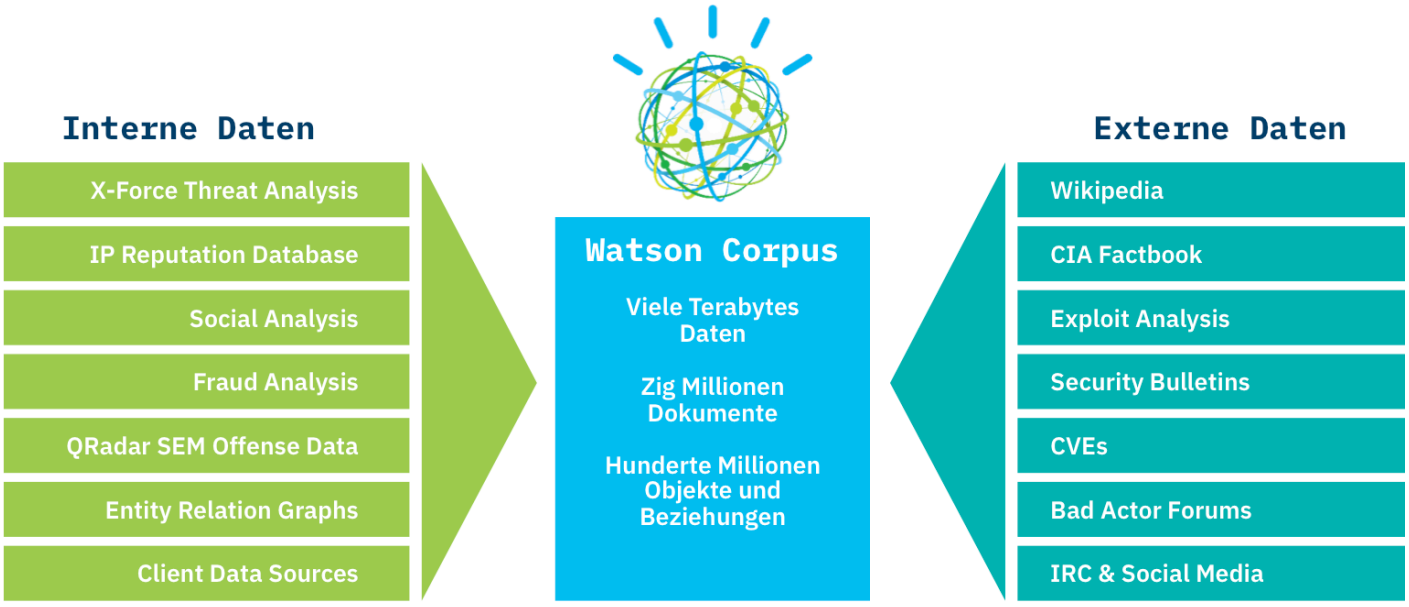

Abbildung 1: Die IBM Watson® for Cyber Secuity Grundstruktur – Analyse Hunderter interner und externer Datenquellen

Die IT-Strategie des BMVg sowie die Cybersecurity-Initiative der Bundeswehr sehen die Gründung eines übergreifenden Cyber Security Operation Center (CSOC) beziehungsweise Security Operation Center (SOC) vor. Auch IT-forensische Untersuchungen sind hier vorgesehen.

Ein SOC umfasst mehrere Komponenten und dient als eine Art Kommandozentrale für Cybersicherheit. Hier laufen alle relevanten Informationen aus der IT-Landschaft zusammen und werden korreliert und analysiert. Die Analysten nutzen dabei verschiedene Dashboards, welche die relevanten Vorgänge im Netzwerk und in der IT-Landschaft darstellen. Je nach Bedarf lässt sich in die einzelnen Vorgänge hineinzoomen, um weitere Einzelheiten in den Blick zu bekommen. Alarme zeigen Auffälligkeiten an, welche die Forensiker mithilfe von Analyse- und Reportwerkzeugen untersuchen können.

Die Einrichtung eines CSOC bzw. SOC kann auch für andere Behörden als Modell dienen, um präventiv und reaktiv wirkende Schutzmaßnahmen nach dem Stand der Technik zu etablieren. IBM Technologie und Beratungsleistungen schaffen hierfür die Prozesse und Infrastrukturen.

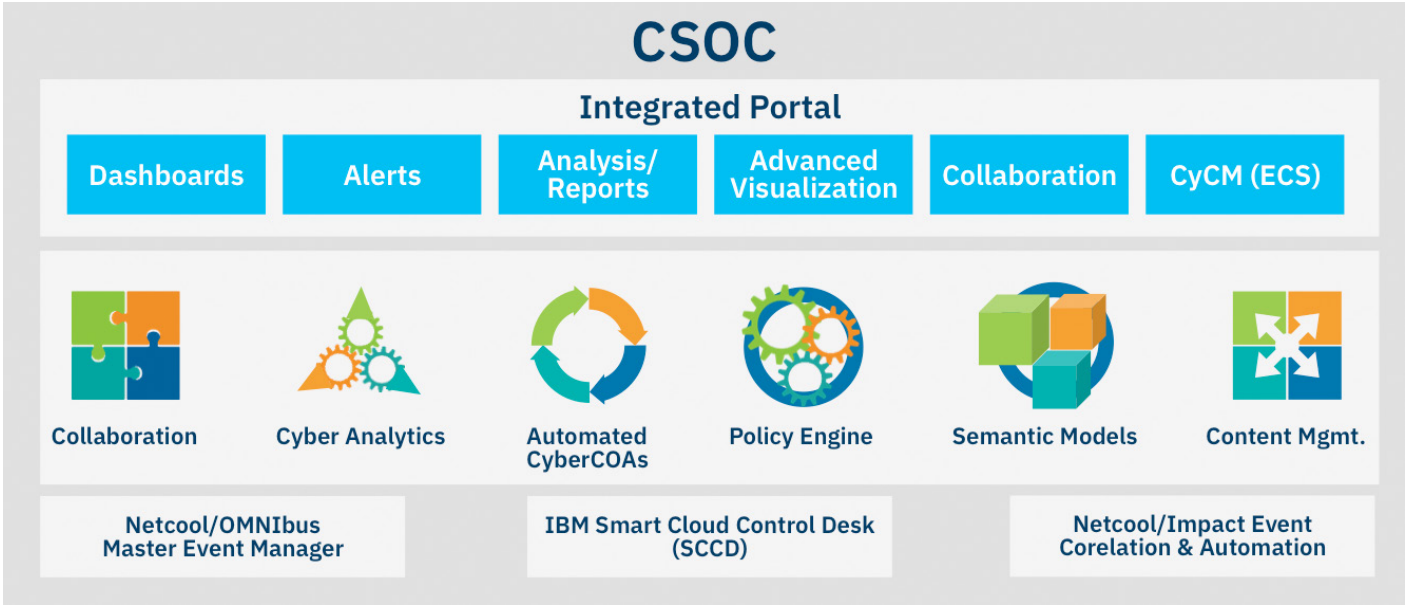

Abbildung 2: Aufbau eines Cyber Security Operation Center (CSOC)

Immer am Ball bleiben – zur Weiterentwicklung der föderalen Sicherheitsarchitektur

Die Anforderungen an die öffentliche Sicherheit steigen stetig. Die Ursache hierfür liegt unter anderem an den immer neuen Wellen an Daten und Informationen, die auf die Behörden zurollen. Anderseits sind die Sicherheitsexperten in Behörden angesichts der vielen Aufgaben zunehmend überlastet.

IBM unterstützt bei der Modernisierung, um mehr Effizienz zu erreichen, sowohl des Informationsverbundes als auch des einzelnen Bediensteten.

Arbeitsteilung durch serviceorientierte Architekturen
Ein Ziel der Modernisierung besteht darin, schnell die Arbeitsweise der Verbundpartner zu erleichtern. Notwendig dafür ist mehr Arbeitsteilung zwischen den Behörden sowie mit externen Partnern. Die Grundlage dafür ist ein Wandel hin zu mehr Serviceorientierung. Beratung bei Transformationen dieser Art zählen zu den Kernkompetenzen von IBM.

Die Vorteile von mehr Arbeitsteilung im Cyber-Umfeld durch Serviceorientierung liegen auf der Hand: Behörden könnten trotz begrenzter Ressourcen Ausfälle kritischer Infrastrukturen vorbeugen. Auch den Kampf gegen die Kriminalität könnten sie verstärken. Gerade kognitive beziehungsweise KI-Systeme leisten hier wertvolle Dienste. Unter anderem helfen sie, Angriffe früher zu erkennen und das Zusammenspiel der Abwehr zu orchestrieren.

Unbedingt notwendig: intelligente Analysen
Ein wichtiger Teil der Modernisierung besteht in neuen, intelligenten Analyse-Instrumenten. Sie helfen vor allem dabei, die Informationen aufzubereiten und zu verdichten. Zudem sind diese Instrumente lernfähig, lassen sich also schnell an Führungs- und Entscheidungsprozesse – zum Beispiel der Polizei – anpassen.

Bleiben wir beim Beispiel der Polizei: Durch vorausschauende Analysen gestützt auf kognitive Analysen und die zentrale Bereitstellung von Informationen wird mehr Prävention bei der Polizeiarbeit möglich. Schnellere Ermittlungen werden zu einer spürbaren Entlastung der Mitarbeiter führen.

Vor allem bei der Auswertung unstrukturierter Daten sowie von Multimedia- und Metadaten leisten kognitive Ansätze große Dienste. IBM bietet in diesem Bereich viele Lösungen, die sich in die hybride Applikationslandschaft eines Behördenverbunds nahtlos einbetten lassen.

Silos aufbrechen – neuer Umgang mit Informationen
Aktuelle Informationen sind der Treibstoff für die Sicherheitsarbeit. Daher muss die historisch gewachsene Informationslandschaft, zumeist zersplittert in Silo- beziehungsweise Registeranwendungen, überarbeitet werden. Die Brücke in die neue Welt bildet ein einheitliches Zugriffs- und Berechtigungsmanagement: Daten für berechtigte Ressorts (beispielsweise Zentralstelle oder Staatsanwaltschaft) werden dabei zugänglich und in einer Art und Weise aufbereitet, dass sie nicht mehr physisch transportiert werden müssen. Die Speicherung und Archivierung von multimedialen Massendaten sollte dabei in zentralen Objektspeichern unter Einhaltung der höchsten Sicherheits- und Datenschutzstandards erfolgen.

Der intelligentere Umgang mit aufbereiteten Informationen und deren föderalen Verarbeitung ermöglicht so auch massive Einsparungen insbesondere bei den Betriebs- und Entwicklungskosten.

Cloud-Plattform für Zusammenarbeit

Der Aufbau einer (Private) INPOL-Community-Cloud bietet die Flexibilität bei der Einbindung neuer Services in die existierende Anwendungslandschaft. Das INPOL-Community-Cloud Vorgehen schafft darüber hinaus Entlastungen für alle Verbundpartner in den Bereichen Anwendungsentwicklung, Test, Rollout und Betrieb. Einheitliche Standards auf höchstem Sicherheitsniveau erlauben jedem Partner eine Integration nach deren freiem Ermessen. Über diese Plattform werden neue Services zeitnah bereitgestellt und in deren lokales Fachverfahren eingebunden.

Die Bildung von Kompetenzzentren, das arbeitsteilige Vorgehen und das aktive Einbringen von Expertenwissen und langjährigen Erfahrungen erlauben mehr fachliche Fokussierung. Neuerungen der Zentrale stehen in wenigen Tagen allen Beteiligten zur Verfügung und erfordern keinen großen Adaptionsaufwand bei den Partnern.

Fazit: Bereit sein für Veränderungen

Am Thema Sicherheit entscheidet sich, ob die Digitalisierung der Behörden ein Erfolg wird oder nicht. Wenn die Bürger und Gewerbetreibende nicht das Gefühl haben, dass ihre Daten bei ihren Ämtern sicher sind, werden sie kein Vertrauen in E-Government-Prozesse oder sonstige Initiativen fassen. Daher muss das Thema mit Priorität angegangen werden.

Eine Alternative dazu gibt es nicht, dafür prescht der Wandel zu schnell voran. Um die Massen an Daten, die Anforderungen an Datenschutz, die kriminellen Energien der Cybercrime-Täter überhaupt zu bewältigen, benötigen Behörden modernste Sicherheitstechnologie – inklusive Servicemanagement, Analytics, KI und Cloud-Infrastrukturen.

Die gute Nachricht dabei: Durch die Modernisierung haben die Behörden die Möglichkeit, neues Potenzial in Sachen Sicherheit zu erschließen. Vorausschauende, proaktive Maßnahmen rücken in den Bereich des Möglichen. Und damit lassen sich nicht nur die augenblicklichen Drohungen abwenden, sondern ihr Schadpotential in Zukunft sogar verringern. Und das sind gute Aussichten.

Und was können wir für Sie tun? Wir freuen uns auf den Kontakt mit Ihnen!

IBM Marketing Öffentlicher Sektor
Mag. Elisabeth Hoelbl
Telefon: +43 6646185805
E-Mail: elisabeth_hoelbl@at.ibm.com

Weitere Informationen finden Sie außerdem im IBM IT Kompass für den öffentlichen Sektor: https://www.ibm.com/industries/de/de/public/e-government.html

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de