eGovernment
COMPUTING
Nr. 02/2017
30. Januar 2017

Sonderdruck zum Thema
Cyber-Sicherheit

bridging IT
Menschen Methoden Lösungen

Cyber-Sicherheit

Risikominimierung und Kosten in vertretbarem Verhältnis

Der öffentliche Bereich gerät unter Druck, die Verfügbarkeit des Cyber-Raums und die **Integrität, Authentizität und Vertraulichkeit** der darin gespeicherten und bewegten Daten soweit wie möglich zu schützen. Die Bundesregierung spricht von einer zentralen gemeinsamen **Herausforderung für Staat, Wirtschaft und Gesellschaft** im nationalen und internationalen Kontext.

Was Behörden tun sollten, um ihren Teil zu mehr Cyber-Sicherheit für ihren Handlungsradius sowie für den Staat, die Wirtschaft und die Gesellschaft beizutragen, erläutert Carsten Triebel, Senior Consultant beim Beratungshaus BridgingIT, im Interview.

Wie dringlich sind die Maßnahmen im Behördenbereich, um sich besser vor Attacken aus dem Cyber Space zu schützen?

Triebel: Der Bedarf ist hier ausgesprochen hoch, zumal in vielen Behörden in puncto Sicherheit hoher Nachholbedarf besteht. Doch es geht hier nicht nur um geeignete Sicherheitssysteme und -werkzeuge, um sich besser vor Angriffen aus dem Cyber-Raum zu schützen. Mehr Cyber Security zu erreichen, das ist vor allem eine organisatorische Herausforderung. Für die Entscheider heißt das, das notwendige Maß an mehr Sicherheit im Gesamtkontext zu sehen.

So müssen die Maßnahmen nachvollziehbar sein, um ihre Wirksamkeit für Governance und Compliance jederzeit nachweisen zu können. Auditing & Reporting vorerst als organisatorische und inhaltliche Maßnahmen spielen in diesem Kontext ganz wichtige Rollen.

Sie sprechen von einem „notwendigen Maß". Wie viel Cyber Security muss sein?

Triebel: Das ist von der Größenordnung des Nachholbedarfs in den einzelnen Behörden abhängig, wobei Cyber Security nur annähernd erreichbar ist. Das hat viele Gründe. Bei technologisch hochentwickelten Schadprogrammen beispielsweise, sind Abwehr- und Rückverfolgungsmaßnahmen schwierig, zumal die Identität der Angreifer aus dem Cyber-Raum und ihre vorrangigen Angriffsziele meist im Dunkeln bleiben. Denn welcher Gruppe – Kriminelle, Terroristen, Nachrichtendienste, Militärs – die Angreifer auch zugehören, sie wollen, dass sie und ihre Absichten solange wie möglich unentdeckt bleiben. Ihre Intentionen werden durch neue Angriffsformen wie Advanced Persistent Threats (APTs) gestützt. Dieser Schadcode wird, nachdem er eingeschleust wurde, oft erst nach vielen Monaten aktiv. Erst ab dann werden für die Behörden kritische Daten abgezogen oder tragende Systeme sabotiert.

Das können Behörden angesichts der wachsenden Gefahr keinesfalls tolerieren. So werden nach dem Analystenhaus Gartner im Jahr 2020 Unternehmen und Organisationen 60 Prozent ihres Sicherheitsetats darauf verwenden müssen, solche verdeckten Attacken aufzuspüren, um schnell und angemessen darauf reagieren zu können.

Wie wichtig sind die Daten für die Angreifer?

Triebel: Mit der voranschreitenden Digitalisierung und Vernetzung haben auch die Daten der Behörden für die Angreifer an Bedeutung gewonnen. Eine länderübergreifende Integration von Datenbanken, intelligente Datenanalysen und -auswertungen sowie ein übergreifender Informationsaustausch motivieren Kriminelle, Terroristen, Nachrichtendienste und Militärs zusätzlich, zu attackieren. Dabei geht es den Angreifern nicht nur

darum, immer aussagekräftigere und vitalere Informationen abzugreifen. Mit der voranschreitenden Digitalisierung, Vernetzung, Datenintegration und -auswertung sowie dem umfassenden Informationsaustausch ist die Abhängigkeit der Behörden von der Informations- und Kommunikationsinfrastruktur gewachsen. Dementsprechend verheerend sind die Folgen, wenn Verwaltungsabläufe durch Schadprogramme oder andere Attacken lahmgelegt oder behindert werden.

Was sollten Behörden tun, um das notwendige Maß an Cyber Security zu ermitteln?

Triebel: Dazu müssen die Entscheider den Status quo an bisher konventionell herausgebildeter IT-Sicherheit genau kennen. Diesen Status fördert eine gründliche Analyse und Bewertung zutage. Aufbauend auf diesem Status quo sollte das Soll an notwendiger Cyber-Sicherheit ermittelt werden. Penetrationstests, die die für die Behörde wichtigsten Bedrohungsszenarien abbilden, leisten dafür hervorragende Dienste.

Danach können die Entscheider die Gefahren für die Verwaltungsabläufe und -tätigkeiten besser bemessen, indem die potenziellen Risiken analysiert, bewertet und qualifiziert werden. Außerdem können Behörden nur mit diesem Wissen unterscheiden, welchen Risiken entgegengewirkt werden sollte und welche Risiken, weil eher vernachlässigbar, toleriert werden können. Nur die Risiken der ersten Kategorie müssen über ein professionelles Risikomanagement überwacht und verfolgt werden.

Sie sprechen damit auch die Leistbarkeit der zu treffenden Maßnahmen an?

Triebel: Ja, Risikominimierung und die Kosten dafür müssen in einem für die Behörde vertretbaren Verhältnis stehen. Zumal für einen hinreichenden Schutz vor Attacken aus dem Cyber-Raum nicht nur geeignete Sicherheitsmaßnahmen und -werkzeuge vonnöten sind.

Ein solcher Schutz muss, neben dem Risikomanagement, auch alle notwendigen Maßnahmen und Werkzeuge für Governance und Compliance im Sinne einer gesamtheitlichen Lösung einschließen. Außerdem bewahrt das Gebot „nicht mehr als notwendig“ die Behörden vor einer zu hohen Komplexität der Gesamtlösung. Weniger komplex, das heißt auch, die Mitarbeiter können die neuen Bedrohungsszenarien und deren Risiken besser nachvollziehen und angemessen darauf reagieren. Beides ist schon deshalb wichtig, weil Cyber Security aus organisatorischer Sicht betrachtet einem kulturellen Wandel gleichkommt. Er muss von den Mitarbeitern unterstützt durch flankierende Schulungs- und Sensibilisierungsmaßnahmen sowie geeignete Richtlinien, Methoden und Werkzeuge gemeistert werden. Von den Mitarbeitern wird es weiterhin abhängen, welche Schutzwirkung der Abwehrschirm entfalten wird.

Welche Hilfestellungen können Richtlinien auf dem Weg zu einem notwendigen Maß an Cyber Security leisten?

Triebel: Das IT-Sicherheitsgesetz des Bundesamts für Sicherheit in der Informationstechnik gibt für den IT-Grundschutz Mindestsicherheitsstandards, Vorgehensweisen und Templates vor, ebenso Methoden wie zertifizierte Audits und Reporting-Prozesse. ISO-Normen, ISMS-Audits, Secure Development Lifecycles sowie Richtlinien und Methoden für mehr Netzwerksicherheit sind weitere wertvolle Hilfestellungen nicht nur für den Werdegang der Cyber Security-Lösung, sondern auch später für deren Betrieb, nicht zu vergessen ITIL als Best-Practice-Modell. Denn am Ende des Werdegangs und am Anfang des Einsatzes steht ein prozessorientiertes IT-Service-Management-System mit einem Information-Security-Management-System als wesentliche Säule darin für eine koordinierte Abwehr von Attacken aus dem Cyber-Raum.

Was sollten Behörden für den technischen Ausbau ihres Schutzschirms bedenken?

Triebel: Die Basis dafür bildet der Status quo der bereits herausgebildeten konventionellen IT-Sicherheit. Zumal einzelne Systeme und Werkzeuge darin wie Identity and Access Management, Intrusion Detection /Prevention Monitoring, Security Event-Korrelation und -Analyse, Verschlüsselung und Secure eMail, sofern vorhanden und angemessen ausgebaut, auch für Cyber-Sicherheit von großer Bedeutung sind. Für eine gezielte Komplettierung zu einem Cyber-Schutzschirm sind weitere Systeme und Werkzeuge gefordert. Dazu zählen Perimeter & Endpoint Security, Mobile Device Security, Advanced Persistent Threat Defense, Vulnerability Testing /Vulnerability Management, Penetration Testing, Security Intelligence sowie natürlich ein professionelles Risikomanagement. Für die richtige Dimensionierung des Cyber-Schutzschirms mit allen Systemen und Werkzeugen darin hat die Behörde mit der Ermittlung der wichtigsten Bedrohungsszenarien und der Analyse, Bewertung und Qualifizierung in nicht tolerable Risiken wichtige Vorarbeit geleistet. Vorsicht bei der Auswahl geeigneter Systeme und Werkzeuge ist schon deshalb geboten, weil Hersteller und Anbieter in einem expandierenden IT-Sicherheitsmarkt oft mehr versprechen, als sie tatsächlich halten können. Deshalb sollten im Einzelnen die strategische Ausrichtung und die funktionale Abdeckung sowie angesichts fast durchweg proprietärer Lösungsansätze die Anschaffungs-, Integrations-, Betriebs- und Weiterentwicklungskosten kritisch hinterfragt werden.

Behörden haben es somit selbst in der Hand, mehr für ihre Cyber-Sicherheit zu tun. Spricht dafür nicht auch der Blick aufs große Ganze: ein verlässliches Funktionieren von Staat, Wirtschaft und Gesellschaft?

Triebel: Zweifellos. Nicht von ungefähr hat der Staat die Gewährleistung von Sicherheit im Cyber-Raum und die Durchsetzung von Recht und den Schutz kritischer Informations- und Kommunikationsinfrastrukturen zu Hauptanliegen gemacht. So wird laut der Bundesregierung eine Cyber-Sicherheitsstrategie bei verteilter Verantwortung von Staat, Wirtschaft und Gesellschaft nur dann erfolgreich sein, wenn alle Akteure gemeinsam und partnerschaftlich ihre jeweilige Aufgabe wahrnehmen. Denn nur so könne die wirtschaftliche und gesellschaftliche Prosperität für Deutschland bewahrt und gefördert werden.

Das Interview führte Hadi Stiel

Der Gesprächspartner

Carsten Triebel,
Senior Consultant
beim Beratungshaus bridgingIT