KRISENMANAGEMENT UND CYBER-BEDROHUNGEN

Informationssicherheit und Informationssicherheits-Management in Zeiten der Pandemie

| von MORITZ HUBER und JENS WESTPHAL

Die Corona-Krise hat das gesellschaftliche Leben in Deutschland und weltweit in einer Art und Weise verändert, wie es sich nur die Wenigsten hätten vorstellen können. Innerhalb kürzester Zeit haben Gesellschaft, Wirtschaft und öffentliche Einrichtungen ihr Zusammenleben und -arbeiten neu organisiert. Unternehmen und Behörden haben kreativ und pragmatisch Lösungen für immer neue Herausforderungen gefunden. Jetzt ist es an der Zeit zu konsolidieren und zu optimieren. Denn die in Rekordzeit implementierten Systeme und Prozesse werden Grundlage für weitere Maßnahmen im Umgang mit der Krise sein.

COVID-19: KATALYSATOR DES DIGITALEN WANDELS

Zumindest in einem Punkt scheint das Virus auch einen positiven Effekt zu haben: COVID-19 wirkt als eine Art Katalysator für verschiedenste Digitalisierungsprozesse und das höchstwahrscheinlich über das noch nicht absehbare Ende der Krise hinaus. Es hat zur Verlagerung von vielen Arbeitsplätzen ins Homeoffice geführt. Die Beantragung der kurzfristig beschlossenen Soforthilfemaßnahmen für Unternehmen ist über eilig eingerichtete Internetplattformen erfolgt. Und zur Identifizierung und Unterbrechung von Infektionsketten wurde eine Tracing-App für Smartphones entwickelt.

Die genannten Beispiele haben zwei Gemeinsamkeiten: Zum einen basieren sie auf moderner Informations- und Kommunikationstechnik. Zum anderen wurden die bereits implementierten Systeme und Prozesse unter Hochdruck extrem schnell entwickelt und mit der sprichwörtlichen „heißen Nadel" gestrickt. Dieser Umstand birgt einige Risiken.

KRISENBEWÄLTIGUNG AUF KOSTEN DER SICHERHEIT

Die Bedrohungslage durch Cyberangriffe hat sich deutlich verschärft. Am Beispiel der großflächigen Einrichtung von Homeoffice-Arbeitsplätzen wird die Problematik besonders deutlich. Behörden, die bislang Remote-Zugriffe auf ihre IT-Systeme und Daten restriktiv gehandhabt haben, sind nun Risiken eingegangen, die unter anderen Umständen wohl niemals genehmigt worden wären: Die Nutzung privater Rechner zu dienstlichen Zwecken, Kommunikation über unverschlüsselte Leitungen oder schwach abgesicherte Zugriffsverfahren an der Schnittstelle zwischen den Verwaltungsnetzen und dem Internet sind nur einige besonders kritische Schwachstellen. Und dieser gestiegenen Verwundbarkeit der öffentlichen IT-Systeme stehen global agierende Cyberkriminelle und nachrichtendienstliche Akteure gegenüber. Erste Betrugsversuche sind bekannt geworden und rufen Schlagzeilen der Vor-Corona-Zeit in Erinnerung: Bei den Cyberangriffen auf das Klinikum Neuss[1], das Kammergericht in Berlin[2] oder die Universität Gießen[3] kam es zu langwierigen Systemausfällen und enormen Schäden. Ganz aktuell ist der Angriff auf die Technischen Werke Ludwigshafen[4], bei dem im großen Stil auf Geschäfts- und Kundendaten zugegriffen werden konnte.

UNSICHERE SYSTEME TREFFEN AUF SKRUPELLOSE TÄTER

Dass Hacker und Cyberkriminelle bereit sind, diese neuen Schwachstellen auszunutzen, betonen die Lageberichte der Sicherheitsbehörden. EUROPOL kommt beispielsweise zu dem Ergebnis, dass die Auswirkungen von COVID-19 in keinem anderen Kriminalitätsfeld so spürbar sind wie im Cyberbereich.[5]

Neue Verschlüsselungstrojaner, Phishing-Kampagnen und eine Neuausrichtung der Underground-Economy sind Schattenseiten der Digitalisierung. Die Folge sind Schäden aufgrund krimineller Cyberangriffe, die unter Umständen ganze Behörden lahmlegen und deren Beseitigung dann viel Zeit und Geld kostet. Was also tun?

DIGITALISIERUNG BRAUCHT EINE SUBSTANZIELLE RISIKOANALYSE

Nur digital gestützte Prozesse ermöglichen es, die in der Krise erforderliche Reaktionsgeschwindigkeit zu erreichen, etwa bei der Nachverfolgung von Infektionsketten bei Pandemien und der Benachrichtigung von Betroffenen. Darum ist eine schnelle Digitalisierung notwendig. In der Praxis wird alles, was dabei hinderlich sein könnte, zunächst zur Seite geschoben. So wird zum Beispiel die Absicherung der eilig aus dem Boden gestampften digitalen Prozesse mit Mitteln der Informationssicherheit gerne als ein solches bremsendes Element wahrgenommen – und deshalb vernachlässigt. Die dadurch entstandene mangelhafte Sicherheit bleibt dann langfristig erhalten und stellt permanent Einfallstore für Angreifer bereit.

Wenn digital gestützte Prozesse entstehen, an bestehenden Systemen Veränderungen vorgenommen oder neue Systeme entwickelt werden, müssen zunächst die dabei neu oder zusätzlich entstehenden Risiken identifiziert und zumindest sehr zeitnah gezielt behandelt werden. Das ist eine Aufgabe für erfahrene Spezialisten, die um die Bedrohungsszenarien wissen, sämtliche Schwachstellen erkennen und in einem dynamischen Prozess die richtigen Schlussfolgerungen ziehen. Externe Experten aus spezialisierten Beratungshäusern, Organisationen, CERTs oder Ähnlichem überblicken die technischen und organisatorischen Folgen, können sie einordnen und bewerten und den Prozess bis zur Implementierung eines Informationssicherheits-Managementsystems (ISMS) begleiten.

BASIS GANZHEITLICHER SCHUTZMASSNAHMEN IST EIN MASSGESCHNEIDERTES ISMS

Bereits kurz nach der Jahrtausendwende hatte die Bundesverwaltung erkannt, dass den (damals noch) neuartigen Gefahren aus dem Cyberraum adäquat begegnet werden muss. Ab 2005 wurde dann der Nationale Plan zum Schutz der Informationsinfrastrukturen (NPSI) formuliert, der mit dem Umsetzungsplan (UP) Bund 2007 konkretisiert wurde. Im Juli 2017 hat das Bundeskabinett eine Neufassung des UP Bund beschlossen. Dies ist die heute gültige Leitlinie zur IT-Sicherheit in der Bundesverwal-

tung.[6] Der UP Bund setzt verbindliche Rahmenbedingungen für den Schutz der in der Bundesverwaltung verarbeiteten Informationen und der dazu genutzten Systeme, Dienste und Infrastrukturen. Er verpflichtet die Behörden zu einem nachhaltigen und standardisierten Informationssicherheitsmanagement (ISMS) und zur Sicherstellung eines angemessenen Sicherheitsniveaus. Solche ISMS sind heute in der Bundesverwaltung noch nicht überall vorhanden beziehungsweise wirksam. Institutionen jedoch, die über ein funktionsfähiges ISMS verfügen, das zudem auf die jeweils spezifischen Belange zugeschnitten ist, sind bei gleichbleibend hohem Sicherheitsniveau schneller in der Reaktion und Anpassung als Häuser ohne ISMS.

AUCH DYNAMISCHE PROZESSE UND AGILE ENTWICKLUNGEN KÖNNEN SICHER GESTALTET WERDEN

Ein wesentliches Merkmal eines ISMS ist seine Fähigkeit zur Erneuerung und Berücksichtigung von Entwicklungen, die beim ursprünglichen Aufbau dieses ISMS noch nicht abzusehen waren. Dafür ist es von Zeit zu Zeit erforderlich, die grundlegenden Paradigmen des ISMS zu überprüfen. Dies gilt insbesondere jetzt in der Krise: Die im Einsatz befindlichen ISMS müssen unter Berücksichtigung der veränderten Bedrohungslage nachjustiert werden. Das beinhaltet etwa organisationsspezifische Maßnahmen, die eine dynamische Reaktion auf krisenartige Entwicklungen ermöglichen. Beispielsweise kann der Aufbau von Krisenreaktionsteams (auch organisationsübergreifend) oder das Vorhalten von Equipment für sicheres Remote-Arbeiten erforderlich sein. Zumindest müssen Pläne erstellt und geprobt werden, um in der Krise die Verfügbarkeit operativer Prozesse zu erhalten oder schnell wiederherzustellen.

Doch auch jenseits der Krise sind Anpassungen möglich und nötig. So wurden in der Bundesverwaltung in den letzten Jahren in Ergänzung zum klassischen V-Modell XT auch agile Entwicklungsumgebungen geschaffen. Ein darauf zugeschnittenes ISMS kann Einfluss auf die Sprints agiler Projekte nehmen und diese gegebenenfalls verhindern, wenn die IT-Sicherheit eines Inkrements (zu weit) von den Anforderungen abweicht. Im Ergebnis können sich Fehler in konzeptionellen Vorgaben oder deren Umsetzung gar nicht erst einschleichen. Damit sind auch für agile Prozesse in der Softwareentwicklung die Regeln auf Grundlage des ISO-Standards 27034-3 (Application Security Management Process) umgesetzt.

RISIKOBEGRENZUNG DURCH KOSTEN-NUTZEN-ANALYSE

Empfehlenswert ist ein standardisiertes Vorgehen zum Umgang mit Risiken, das sich an der ISO 31000 orientiert, dabei aber die für schnelle Reaktionen notwendigen Abkürzungen innerhalb der Norm nimmt. Die ISO 31000 legt Wert auf Vollständigkeit, lässt aber auch Freiräume in der Ausgestaltung und Umsetzung. Darüber hinaus ist es möglich, den Risikomanagementprozess an andere bestehende Managementsysteme anzulehnen und damit von Erkenntnissen zu profitieren, die in der Organisation bereits vorhanden sind. Der ganzheitliche Ansatz betrachtet IT-Risiken nicht isoliert, wie es beispielsweise bei einem Vorgehen nach ISO 27005 oder BSI 200-3 geschieht. Vielmehr werden generalisierte unternehmerische Risiken, die innerhalb der IT wirksam werden, in der Gesamtsicht bewertet und quantifiziert. Auf diese Weise werden Risiken minimiert, ohne dass der dafür betriebene Aufwand (zeitlich und finanziell) den angestrebten Nutzen übersteigt. ●

Moritz Huber beschäftigt sich als Kriminalbeamter, Wirtschaftsinformatiker und Dozent schon viele Jahre mit dem Thema Sicherheit aus unterschiedlichen Perspektiven. Derzeit leitet er die Zentrale Ansprechstelle Cybercrime (ZAC) im Landeskriminalamt Baden-Württemberg und promoviert zudem am „The Open Government Institute (TOGI)" der Zeppelin Universität im Themenfeld „Smart Security".

1 https://www.kma-online.de/aktuelles/klinik-news/detail/900000-euro-gesamtschaden-durch-cyberattacke-a-31629 (abgerufen am 15.07.2020).
2 https://www.tagesspiegel.de/berlin/cyberangriff-auf-berliner-kammergericht-russische-hacker-koennten-justizdaten-gestohlen-haben/25477570.html (abgerufen am 15.07.2020).
3 https://www.forschung-und-lehre.de/politik/uni-giessen-nach-cyberangriff-groesstenteils-wieder-online-2652/ (abgerufen am 15.07.2020).
4 https://www.ludwigshafen24.de/ludwigshafen/ludwigshafen-hacker-twl-deutschland-angriff-technische-werke-strom-kunden-daten-passwort-gefahr-13748874.html (abgerufen am 15.07.2020).
5 https://www.bild.de/news/ausland/news-ausland/wegen-corona-europol-warnt-cybercrime-betrug-und-diebstahl-nehmen-zu-69658798.bild.html (abgerufen am 15.07.2020).
6 https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html (abgerufen am 15.07.2020).