Sich gegen Risiken umfassend wappnen

Business Continuity Management (BCM) soll das Überleben einer Unternehmung im Notfall sicherstellen. Die Schweiz und die EU verschärfen die Anforderungen an die Cybersicherheit. Unternehmen müssen deshalb auch den Cybernotfall abdecken, denn er wird immer wichtiger.

AUTOR

Prof. Dr. Richard Werner

Future Intelligence Group AG, Chief Executive Officer & President of the Board Head office, Neerach.

> *future-intelligence.ch*

Von **Richard Werner**

Die Zahl der Cyberangriffe nimmt zu. Nach Angaben des Nationalen Zentrums für Cybersicherheit (NCSC) wurden dem Kompetenzzentrum des Bundes seit Jahresbeginn mehr als 13 000 Hacking-Vorfälle gemeldet. Betroffen sind unter anderem NZZ, CH Media, SBB und verschiedene Technologiekonzerne. Auch haben die Cyberkriminellen Daten, darunter heikle Personendaten der Bundesverwaltung, im Juni vollständig im Darknet veröffentlicht. Unter den Daten finden sich Offerten, Kundendaten, Mailkorrespondenzen, Projekte, Namen und Ordner von Mitarbeitenden. Auch Kantone wie der Aargau sowie das Bundesamt für Polizei (Fedpol) sind davon betroffen.

Schlechter Zeitpunkt

Während eines Notfalls ist der schlechteste Zeitpunkt, um festzustellen, dass das Business Continuity Management der Organisation ungeeignet ist. Nachfolgend wird eine einfache Methode gezeigt, um die Reaktionsfähigkeit eines BCM zu überprüfen, um den Fortbestand des Unternehmens zu sichern.

1. In Stresssituationen verwenden

Je komplexer das BCM-Handbuch ist, desto länger dauert es, bis die Verantwortlichen entscheiden können, welches Szenario man anwenden will. Dadurch verzögert sich nicht nur die Reaktion, sondern man hat möglicherweise auch noch nicht alle relevanten Informationen erhalten. Mit anderen Worten: Eine anfängliche Entscheidung muss möglicherweise später noch einmal überdacht werden, während die Verantwortlichen noch unter Stress stehen.

2. Parameter bei Bedarf anpassen

Wenn die Informationen eintreffen und das Notfallmanagement greift, können und werden sich die Umstände ändern. Die Probleme sind vielleicht nicht so schlimm wie ursprünglich befürchtet, einige Reaktionen haben nicht so gut funktioniert wie erwartet, Ressourcen stellen sich als nicht vorhanden heraus – wenn die Verantwortlichen sich auf ein zu präskriptives Szenario festlegen, können sie sich nicht flexibel anpassen.

3. Szenarien müssen geübt werden

Je weniger und je flexibler die Notfallmanagementszenarien eines bestimmten Unternehmens sind, desto einfacher ist es, sie in Schulungen zu üben. Solche IT-Notfallübungen oder IT-Krisenstabsübungen ermöglichen eine Feinabstimmung, die Korrektur falscher oder veralteter Aspekte, schaffen Vertrauen in den Prozess und machen ihn vertraut.

All dies reduziert den Stress, wenn es an der Zeit ist, diese Szenarien in der Realität auszuführen, was wiederum zu weniger Fehlern bei der Ausführung und weniger rechtlichen Risiken führt.

Die Zeiten werden sich in der IT komplett ändern

Mit dem Digital Operational Resilience Act (Dora) oder der NIS-2-Richtlinie («The Network and Information Security Directive) müssen Finanzdienstleister die Widerstandsfähigkeit (Resilienz) und Reaktion auf Sicherheitsvorfälle und gegen betriebliche Störungen auf der IT-Ebene beweisen. Dabei geht es um Cybersecurity und externe Angriffe, aber auch um eine Reihe anderer, nicht böswillig verursachter, schwerwiegender IT-Probleme.

Ab 2024 müssen Unternehmen aus 18 Branchen mit mehr als 50 Mitarbeitern und 10 Millionen Euro Umsatz ein dediziertes Cybersicherheitsmanagement einführen.

Mit einer Ausweitung der Sektoren auf insgesamt 18 NIS2-Sektoren (Kritische Bereiche wachsen bis zu 11 Sektoren, wichtige Bereiche auf bis zu 7 Sektoren an) werden allein in Deutschland rund 29 000 Unternehmen und Institutionen von den neuen europäischen Regelungen für kritische Infrastrukturen betroffen sein. Das bedeutet, dass künftig auch viele neue Unternehmen den Regulierungen unterliegen, die bisher nicht zu den Betreibern kritischer Infrastrukturen gezählt wurden.

In Zukunft müssen Unternehmen beispielsweise auch Risiken durch Leistungen von Drittanbietern in ihren Analysen berücksichtigen, etwa solche von Cloud-Dienstleistern. Dazu kommen gemäss

© depositphotos, Sergey Nivens

Business Continuity Management bedeutet auch, den Cybernotfall abzudecken, denn das Geschäft der Hacker floriert.

Dora-Vorgaben zur Meldung von Änderungen in der Nutzung von IKT-Anbietern, detailliertere Regeln für die durchzuführenden Prüfungen und Penetrationstests sowie die Benennung aller in Anspruch genommener sogenannter «kritischer Drittanbieter».

Laut Dora werden folgende Tests durchgeführt: «Durchführung eines vollständigen Spektrums geeigneter Tests, darunter Bewertungen und Überprüfungen der Anfälligkeit, Analysen von Open-Source-Software, Bewertungen der Netzsicherheit, Lückenanalysen, Analysen der physischen Sicherheit, Überprüfungen der physischen Sicherheit, Fragebögen und Scansoftwarelösungen, Quellcodeprüfungen soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests oder Penetrationstests.» Die Resultate dienen dann als Vorgabe für alle notwendigen Wiederherstellungsmassnahmen. Hierbei besteht die Herausforderung, die tatsächlichen Wiederherstellungszeiten zu erproben, zu dokumentieren und transparent zu machen, und das über die ganze Abhängigkeitskette der Geschäftsprozesse hinweg. Die Ergebnisse sind der zuständigen Finanzbehörde zu melden.

Der bisherige Anwendungsbereich der NIS-Richtlinie nach Sektoren wird mit NIS2 auf einen weit grösseren Teil der Wirtschaft ausgeweitet, um eine umfassende Abdeckung der Sektoren und Dienste zu gewährleisten, die im Binnenmarkt für grundlegende gesellschaftliche und wirtschaftliche Tätigkeiten von entscheidender Bedeutung sind.

Betroffene Einrichtungen müssen daher geeignete Risikomanagementmassnahmen für die Sicherheit ihrer Netz- und Informationssysteme treffen und unterliegen Meldepflichten.

Wer ist betroffen?

Betroffen sind grosse und mittlere Unternehmen aus diversen Sektoren. Wesentliche Einrichtungen sind: Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Wasser- und Abwasserversorgungen sowie andere mehr.

Wichtige Einrichtungen sind: Post- und Kurierdienste, Abfallbewirtschaftung, Chemie, Lebensmittelversorger, verarbeitendes/herstellendes Gewerbe oder Anbieter digitaler Dienste.

Betroffen sind vereinzelt aber auch kleine Unternehmen mit weniger als 50 Mitarbeitenden. Folgende Unternehmen fallen unabhängig von ihrer Grösse in den Anwendungsbereich: Vertrauensdiensteanbieter, Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste, TLD-Namenregister und DNS-Dienste-anbieter, ausgenommen Betreiber von Root-Namenservern, Unternehmen, die alleiniger Anbieter eines Service in einem Staat sind, der essenziell für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten ist. Zusätzlich müssen auch Dienstleister und Lieferanten von betroffenen Unternehmen Sicherheitsvorkehrungen einhalten.

Was gibt die Richtlinie vor?

Es sind Risikomanagementmassnahmen zu treffen und Berichtspflichten zu beachten. Die Leitungsorgane (Geschäftsführer bei GmbH, Vorstände bei Aktiengesellschaft) überwachen die Umsetzung und haften bei Verstössen.

Welche Massnahmen sind zu treffen?

Es gilt, mindestens zehn Risikomanagementmassnahmen zu berücksichtigen:

- Konzept Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Business Continuity und Krisenmanagement
- Sicherheit der Lieferkette
- Sicherheitsmassnahmen bei Erwerb/Entwicklung/Wartung von IKT
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmassnahmen
- Cyberhygiene und Schulungen zur Cybersicherheit
- Kryptografie und ggf. Verschlüsselung
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle

- Multi-Faktor-Authentifizierung
- Cybersecurity

Dabei zu berücksichtigen sind:

- der Stand der Technik
- europäische und internationale Normen
- Kosten der Umsetzung
- bestehendes Risiko

Bei der Bewertung der Verhältnismässigkeit dieser Massnahmen sind das Ausmass der Risikoexposition der Einrichtung, die Grösse der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere einschliesslich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen.

Was passiert bei Regelverstoss?

Bei Nichterfüllung drohen Sanktionen bis zu 10 Millionen Euro oder 2 Prozent des Gesamtjahresumsatzes des Konzerns bei wesentlichen Einrichtungen beziehungsweise 7 Millionen Euro oder 1,4 Prozent des Gesamtjahresumsatzes des Konzerns bei wichtigen Einrichtungen.

Leitungsorgane (Geschäftsführer und Vorstand) haften für Verstösse, wenn essenzielle Risikoabwägungen vernachlässigt oder ignoriert wurden.

Handlungsfähigkeit auch nach einem Katastrophenfall

Unter Business Continuity Management wurde noch vor wenigen Jahren vor allem ein Werkzeug verstanden, das darauf abzielt, IT-Systeme (und damit in vielen Fällen indirekt auch die Produktion) neu zu starten und verlorene Daten und Anwendungen wiederherzustellen (im Sinne einer IT-Disaster-Recovery-Planung). Infolgedessen ist die Wahrnehmung der IT-Neustart- und Wiederherstellungszeiten in Industrieunternehmen eher technologieorientiert.

Grundlegende Wertschöpfungsprozesse sind jedoch in der Regel nicht Gegenstand der BCM-Analyse. Darüber hinaus ist es aufgrund der isolierten Betrachtung oft nicht möglich, die vollständigen wirtschaftlichen Folgen einer Betriebsunterbrechung abzuschätzen. Heute setzt sich jedoch – zumindest bei grossen internationalen Industrieunternehmen – ein ganzheitlicher Ansatz durch. Im Vordergrund steht die Betrachtung und finanzielle Bewertung der Auswirkungen auf alle gewinnkritischen Prozesse. Der Zweck des Business Continuity Management besteht darin, den Geschäftsbetrieb aufrechtzuerhalten und so einen Mehrwert zum Schutz des Unternehmens (u.a. Reputation und Marke) zu gewährleisten, aber auch die Interessen der Aktionäre wahrzunehmen. Für BCM stehen Risiken mit einem sehr hohen Schadenspotenzial im Vordergrund, während die Eintrittswahrscheinlichkeit zweitrangig ist, da immer davon ausgegangen werden muss, dass der Eintrittszeitpunkt jederzeit sein kann.