REDEN WIR ÜBER AUFSICHT

KOMPLEXE VORGABEN.
KLARE ERWARTUNGEN.

FMA

IKT-Risikomanagement unter DORA

Erfahrungen aus der Aufsichtspraxis

Im Rahmen von DORA spielt das IKT-Risikomanagement eine zentrale Rolle für die Steuerung von IKT-Sicherheitsmaßnahmen. Ist der Prozess mangelhaft oder wird das Risikomanagement bei der Beschaffung von Sicherheitslösungen und der Einführung von Sicherheitsmaßnahmen nicht berücksichtigt, dann drohen Ineffizienzen und Fehlinvestitionen. Ein Risiko, das im Rahmen von Vor-Ort Prüfungen der FMA behandelt wird.

DORA
Der Digital Operational Resilience Act der EU zielt darauf ab, die Cybersicherheit und operationale Widerstandsfähigkeit des Finanzsektors zu stärken. Der Rechtsakt ist seit 17. Januar 2025 vollständig anwendbar.

Im Rahmen von DORA versteht man unter dem IKT-Risikomanagement die Strategien, Maßnahmen und Verfahren, die Finanzunternehmen zur Identifikation, Bewertung, Steuerung und Minderung von Risiken im Zusammenhang mit Informations- und Kommunikationstechnologien (IKT) einsetzen. DORA sieht dabei insbesondere das Leitungsorgan in der Pflicht. Daher muss auch die Berichterstattung über das IKT-Risikomanagement so ausgestaltet sein, dass der Vorstand ausreichend informiert ist und auf dieser Basis Entscheidungen z. B. zur Implementierung zusätzlicher Sicherheitslösungen und Maßnahmen treffen kann.

In der Aufsichtspraxis haben sich aus Sicht der FMA einige Themen herauskristallisiert, die zu Missverständnissen und Fehleinschätzungen im Prozess des IKT-Risikomanagements führen können. Außerdem zeigt sich in Vor-Ort-Prüfungen, dass vielfach neue IKT-Sicherheitslösungen und -Maßnahmen unabhängig vom IKT-Risikomanagement implementiert werden. Im Ergebnis weisen Unternehmen bei grundlegenden Prozessen und Kontrollen für die IKT-Sicherheit Mängel auf, investieren aber gleichzeitig in fortschrittliche und teure Sicherheitslösungen, die die Mängel in den grundlegenden Prozessen nicht oder nur eingeschränkt mitigieren können.

Analyse von Schwachstellen

Ein verbreitetes Thema ist die **Analyse von Schwachstellen.** Diese spielen für die Identifizierung der IKT-Risiken eine wesentliche Rolle.
Diese Risiken ergeben sich aus der Kombination von Bedrohungen einerseits und vorhandenen Schwachstellen andererseits, also zusammengefasst aus der Formel **Bedrohungen + Schwachstellen = Risiken**

DORA definiert Schwachstellen hier in einem weiteren Sinn, wie aus den Begriffsbestimmungen der Verordnung hervorgeht. Insbesondere versteht es Schwachstellen nicht nur als technische, sondern berücksichtigt zum Beispiel auch Abläufe oder organisatorische Verfahren.
Betrachten wir als Beispiel das Management von Sicherheits-Softwareupdates:

- Hat eine Software eine Sicherheitslücke, so liegt eine **technische Schwachstelle** im System vor. Diese muss durch das Einspielen eines Patches geschlossen werden.
- Enthält nun der **Prozess des Patch-Management** Mängel, wie zum Beispiel den, dass Sicherheitsupdates nicht oder nicht zeitnah ausgerollt werden, dann ist dies ebenfalls als eine Schwachstelle im Sinne von DORA zu verstehen.
- Auch die **fehlende Definition von Zuständigkeiten** für das Patchen von Systemen, und/oder eine fehlende **nachgelagerte Überwachung** der Ausrollung der Patches, kann als eine Schwachstelle verstanden werden, da sie dazu führen kann, dass Patches nicht auf allen Systemen systematisch und zeitnah ausgerollt werden.

§ **Dora VO Artikel 3 (16)**
»Schwachstelle«: *eine Schwachstelle, Empfindlichkeit oder Fehlfunktion eines Vermögenswerts, eines Systems, eines Prozesses oder einer Kontrolle, die ausgenutzt werden kann*

Ausreichend granulare Risikoidentifikation

Um Schwachstellen in ausreichendem Maße erheben zu können, müssen bereits bestehende IKT-Sicherheitsmaßnahmen im Rahmen der Risikobewertung berücksichtigt werden. Dies kann nur dann erfolgen, wenn sowohl die Risikoidentifikation als auch die Berücksichtigung getroffener Maßnahmen zur Risikoreduktion, in einem ausreichend granularen Format vorliegen, sodass eine Zuordnung der bisher getroffenen Maßnahmen zu den bestehenden Risiken erfolgen kann. Eine ausreichende Granularität ist auch die Grundlage dafür, dass zielgerichtet neue Maßnahmen identifiziert und priorisiert werden können. Zur Beurteilung der Adäquanz der Schwachstellenerhebung ist es erforderlich, die Vorgehensweise in den Kontext von Unternehmensgröße, Komplexität und auch implementiertem Risikomanagement des Unternehmens zu setzen.
Werden Investitionen in teure und komplexe Sicherheitslösungen vorgenommen, obwohl im Unternehmen bekannt ist, dass gleichzeitig Mängel in grundlegenden Sicherheitsprozessen bestehen, kann dies ein Indikator sein, dass die identifizierten Risiken und getroffenen Maßnahmen in keiner ausreichenden Granularität vorliegen. Eine Orientierungshilfe für eine ausreichende Granularität können auch Gefahrenkataloge und Bedrohungslandkarten von anerkannten Best Practice Standards geben.
Darüber hinaus sind zusätzliche Prozesse zu implementieren, die evaluieren, ob

die bestehenden Sicherheitsmaßnahmen effektiv sind. Dazu können zum Beispiel interne oder auch externe Audits sowie Self-Assessments herangezogen werden. Werden dadurch Kontrollen und bestehende Maßnahmen als nicht oder nur eingeschränkt effektiv befunden, ist dies bei der Risikobewertung wiederum zu berücksichtigen, da sich dadurch entweder neue Schwachstellen ergeben können oder das Ausmaß bestehender Schwachstellen erhöht wird.

§ **Art.3 DELVO (EU) 2024/1774**
Seitens der Unternehmen ist sicherzustellen, dass die Wirksamkeit der implementierten Maßnahmen für die Behandlung von IKT-Risiken überwacht wird.

Risikosteuerung & Überwachung

Ergeben sich im Rahmen der Risikobewertung nun Risiken, die über der Risikotoleranzschwelle des Unternehmens liegen, müssen weitere Maßnahmen zur Reduktion des Risikos definiert werden, sofern dies zweckmäßig ist. Dabei sollten die Kosten für die Maßnahmen den potenziellen Schaden bei Eintreffen des Risikos gegenübergestellt werden. Außerdem sollte die Beurteilung einer Maßnahme betreffend ihrer Eignung zur Reduktion eines Risikos durchgeführt werden. Dies führt nach Abschluss der geplanten Maßnahme dazu, dass das Risiko, sofern die Bedrohungslage unverändert ist, niedriger bewertet werden kann.
Diese Risikoanalyse ist wesentlich dafür, dass Geld oder Ressourcen für eine Verbesserung der Risikosituation nicht in die falschen Bereiche wandern. Beispiele zu Mängeln in grundlegenden Prozessen und Kontrollen sind unter anderem ungepatchte oder zu selten gepatchte Systeme, keine oder zu unsichere Passwortrichtlinien für Administratoren oder der zu weitreichende Einsatz von hochprivilegierten Benutzern (Domain Admin, root). Sicherheitsrisiken, die sich aus den angeführten Mängeln ergeben, können oft nur eingeschränkt durch andere Sicherheitsmaßnahmen kompensiert werden. Auch sind die Kosten für kompensierende Maßnahmen oft signifikant höher, als der Aufwand, der sich ergibt, um die eigentlichen Mängel zu beseitigen.
Der IKT-Risikomanagementprozess eines Unternehmens muss als Ziel haben, jene Sicherheitsmaßnahmen zu identifizieren, die den größten Effekt auf die Gesamtrisikosicht, verglichen mit den dafür notwendigen Kosten, haben – somit das beste Kosten-Nutzen-Verhältnis aufweisen.

§ **Art.3 Lit c DELVO (EU) 2024/1774**
Seitens der Unternehmen ist sicherzustellen, dass Maßnahmen für die Behandlung von IKT-Risiken festgelegt werden, die erforderlich sind, um diese unter die festgelegte Risikotoleranzschwelle zu bringen

Berichterstattung

Wesentlicher Bestandteil eines guten IKT-Risikomanagement Systems ist dabei auch die Aufbereitung der bestehenden Risikosituation und der möglichen Maßnahmen zur Risikoreduktion für das Leitungsorgan des Unternehmens. Dieses muss von den Experten so informiert werden, dass die richtigen Entscheidungen getroffen und verantwortet werden können. Durch die Letztverantwortung des Leitungsorgans für das IKT-Risikomanagement, hat dieses auch sicherzustellen, dass Prozesse und Verfahren implementiert sind, die sicherstellen, dass Informationen betreffend

der Risikosituation sowie die getroffenen und zusätzlich möglichen Maßnahmen in ausreichender Form an das Leitungsorgan berichtet werden.
Werden die angeführten Punkte berücksichtigt, schafft dies die Basis für die Implementierung eines effektiven IKT-Risikomanagements, welches es Unternehmen und dessen Leitungsorganen ermöglicht, zielgerichtet und effizient Maßnahmen zur Reduktion von Risiken zu implementieren.

Umgekehrt gilt aber auch: Wenn das Leitungsorgan beispielsweise erkennt, dass hohe Investitionen seitens des Unternehmens zur Mitigation von Sicherheitsrisiken getätigt wurden, während gleichzeitig Berichte vorliegen, dass im Patch-Management Schwachstellen vorliegen, dann muss der Vorstand erkennen, dass kein effektives IKT-Risikomanagment implementiert sein kann. Der Vorstand ist in diesem Fall gefordert, entsprechend zu handeln.

Link

Weitere Informationen zu DORA finden Sie auf der Website der FMA:
www.fma.gv.at → Aufsicht → Querschnittsthemen → DORA

§

Wir stützen unsere Aussagen auf teils komplexe rechtliche Vorgaben, die wir am Rand ausweisen, oder leiten sie davon ab, ohne neues Recht zu schaffen, so dass über die gesetzlichen Bestimmungen hinausgehende Rechte und Pflichten hieraus nicht abgeleitet werden können. Wir formulieren klare Erwartungshaltungen, die sich weitestmöglich auf Rechtsprechung und europäische Auslegungshilfen stützen, i. Ü. aber unsere eigene fachkundige Rechtsauffassung wiedergeben. Wir gehen mit der Zeit, weswegen wir uns die Aktualisierung der angeführten Orientierungshilfen jederzeit vorbehalten.
Obige Aufzählungen stellen keine abschließende Liste dar und sind jedenfalls nur ergänzend und klarstellend zu betrachten.