managing expectations
communications

Checkliste «Cyber Security Reporting»

Gesetzeskonformität

□ Verpflichtet sich das Unternehmen öffentlich zur Einhaltung aller relevanten Gesetze, einschliesslich Cyber- und Datenschutz?

Richtlinien

□ Informiert das Unternehmen öffentlich über ihre Datenschutzrichtlinie bzw. Datenschutzerklärung?

□ Deckt die Richtlinie explizit den gesamten Betrieb ab, einschliesslich Dritter?

Rechenschaftspflicht des Managements und Verwaltungsrates

□ Identifiziert das Unternehmen namentlich eine Person auf Führungsebene oder Vorstandsebene mit übergeordneter Verantwortung für Informationsmanagement und die Cyber-Sicherheit?

□ Ist der Verwaltungsrat oder ein Komitee für Cyber-Sicherheit zuständig?

Information des Verwaltungsrates

□ Informiert das Unternehmen den Verwaltungsrat zu Cyber-Risiken, und wenn ja wie, durch wen und wie oft?

□ Erhält der Verwaltungsrat detaillierte Informationen zur Cyber-/Informationssicherheits-strategie des Unternehmens - einschliesslich der Informationen, die er erhält und wie er die diese Informationen bewertet?

Fähigkeiten und Ressourcen

□ Informiert das Unternehmen über das Vorhandensein eines Cyber- und/oder Informationssicherheitsteam und/oder ein dediziertes Budget?

□ Informiert Unternehmen darüber, dass sich der Verwaltungsrat mit relevanten Brancheninitiativen zur Cybersicherheit befasst und/oder Zugang zu internem oder externem Fachwissen zum Thema Cyber-Sicherheit verfügt?

□ Sucht das Unternehmen aktiv nach solchen Fähigkeiten, wenn Führungspersonen ernannt werden?

Ausbildung

□ Bietet das Unternehmen Schulungen zu Information und / oder Anforderungen an die Cybersicherheit für alle Mitarbeiter?

Prüfung

□ Führt das Unternehmen Audits zu den Informationsrichtlinien und/oder Cybersicherheitsrichtlinien und -systemen durch?

Prozesse und Verfahren

□ Verfügt das Unternehmen über einen Störungsmanagementplan (inklusive Notfallplan) und hat einen Geschäftskontinuitätsplan etabliert?

□ Informiert das Unternehmen zu «Cybersicherheit» als wesentlicher Bestandteil der Risikobewertung/des Geschäftskontinuitätsplans?

Quelle: «PRI – Stepping up Governance on Cyber Security 2018» - What is corporate disclosure telling investors»
by Vaishnavi Ravishankar, Olivia Mooney,Nora Hader

Glossar

Die **Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA)** identifizierte bemerkenswerte Cyber-Bedrohungen in ihrem Bericht über die Bedrohungslandschaft 2018.
Dazu gehören:

1. **Malware**, eine der häufigsten Cyber-Bedrohungen, ist bösartige Software, die entwickelt wurde, um einen Computer oder ein mobiles Gerät ohne Zustimmung zu nutzen.

2. **Webbasierte Angriffe** nutzen webfähige Systeme und Dienste wie Browser, Websites und die IT-Komponenten von Webservices und Webanwendungen. Sie werden häufig mit Malware-Kampagnen kombiniert. Beispiele hierfür sind Webbrowser-Schwachstellen und bösartige URLs.

3. **Angriffe auf Web-Applikationen** richten sich gegen Web-Applikationen, Web-Services und mobile Anwendungen.

4. **Phishing-Angriffe** nutzen Social Engineering, um Endbenutzer dazu zu verleiten, auf einen bösartigen Link zu klicken oder ein Attachment, das es dem Angreifer ermöglicht, auf die Zugangsdaten zuzugreifen und Malware zu installieren.

5. **Spam** ist eines der verbreitetsten Mittel zur Verbreitung von Malware.

6. **Denial of Service (DoS)** Angriffe überfordern Server, Systeme oder Netzwerke mit Datenverkehr und verhindern, dass sie die von legitimen Benutzern verwendet werden. Ein DDoS-Angriff (Distributed Denial of Service) verwendet mehrere infizierte Geräte, um ein gezieltes System zu überfluten.

7. **Ransomware** ist eine Art von Malware, die dazu bestimmt ist, den Zugriff auf Benutzerdateien oder den Computer zu blockieren, bis ein Lösegeld wird gezahlt.

8. **Botnet** besteht aus miteinander verbundenen Geräten, die mit Malware infiziert und von einem Cyberkriminellen ferngesteuert werden. Sie werden für Spam-Kampagnen und DDoS-Angriffe eingesetzt.

9. **Insider-Bedrohung** kann entstehen, wenn ein Insider seinen autorisierten Zugang nutzt, um die Sicherheit seiner Organisation zu gefährden, absichtlich oder unabsichtlich.

10. **Physische Manipulation/Beschädigung/Diebstahl/Verlust** von Geräten kann zu einem Datenverlust führen, z.B. bei aufgebrochenen Geldautomaten und gestohlenen Smartphones.