IT-Bedrohungen im Finanzsektor in Zeiten von Covid-19

Sofortmaßnahmen für Banken und Versicherungen

Die Covid-19-Pandemie entwickelt sich schneller als gedacht zu einer globalen Bedrohung. Diese Krise zwingt Organisationen dazu, Maßnahmen zu ergreifen, um ihren Betrieb weiterhin aufrechtzuerhalten. Ein erfolgreiches Krisenmanagement berücksichtigt jetzt seine Mitarbeiter, Kunden sowie Dienstleister und sorgt für einen ausfallsicheren IT-Betrieb.

	Risiken und Herausforderungen	Unterstützung durch KPMG
1	**Lockdown (1-2 Monate)**	
	— Mitarbeiter verwenden private Endgeräte (BYOD), die nicht mit der Sicherheitsrichtlinie des Unternehmens vereinbar sind. — Unautorisierter Datentransfer führt zu Verstößen in der Informationssicherheit und gegen den Datenschutz. — Kritische Auslagerungen werden nicht zuverlässig vom Dienstleister erbracht, getestet oder dokumentiert.	— Kommunikation und Schulungsangebote für Mitarbeiter im Homeoffice. — Evaluation von Wiederherstellungsstrategien (BIA, BCP, DRP). — Überprüfung der SLAs, Verträge und Testpläne zu geschäftskritischen Auslagerungen, insbesondere im Hinblick auf das BCM.
2	**Restart (3-5 Monate)**	
	— Kriminelle Hacker missbrauchen die Covid-19-Krise für gezielte (Phishing-)Angriffe. — Verhaltensmuster in IT-Netzwerken ändern sich. Erkennungsregeln und Netzwerkanalysen können unzuverlässig reagieren. — Datenschutz und Risikosteuerung müssen an die Ausnahmesituation angepasst werden.	— Management von Informationsrisiken mit Fokus auf sensible Geschäftsbereiche. — Unterstützung von IT Security sowie SIEM/SOC-Teams, um eine schnelle Reaktionszeit auf Vorfälle zu gewährleisten. — Wirksamkeitsprüfung von Datensicherungs- und Wiederherstellungsplänen zur Gewährleistung der Verfügbarkeit.
3	**Grow (länger als 6 Monate)**	
	— Sensible Daten in privaten Netzwerkumgebungen erhöhen das Risiko von Bedrohungen. — Gefahr der Überlastung von IT-Systemen aufgrund mangelnder Skalierbarkeit und Kapazitätsengpässen. — Umgesetzte Sofortmaßnahmen verstoßen gegen regulatorische Anforderungen.	— Einsatz von Cloud-Services für eine skalierbare und nachhaltige Transformation der IT-Infrastruktur. — Evaluation von KI-gestützten SIEM/SO-Lösungen für eine 360 Grad Überwachung des Netzwerkverkehrs. — Einführung einer „Digital Identity“ und von „Behaviour Analytics“ as a Service zur Effizienzsteigerung und Erhöhung der Security.

Die Besorgnis über die Auswirkungen der Covid-19-Pandemie wachsen. IT-Leiter und Informationssicherheitsbeauftragte müssen jetzt über angemessene Maßnahmen entscheiden. Daher ist es ratsam, sich zu fragen, ob Ihr Unternehmen auf ein krisensicheres Arbeiten vorbereitet ist.

Self-Assessment

1. Wurde eine BYOD-Richtlinie definiert und kommuniziert?
2. Werden sensible Unternehmensdaten und Geschäftskommunikation weiterhin sicher übermittelt?
3. Werden SLAs weiterhin eingehalten und müssen Auslagerungen durch das Business Continuity Management angepasst werden?
4. Können Sie Netzwerkanomalien identifizieren und auf potenzielle Störungen zeitnah reagieren?
5. Müssen Datensicherungs- und Wiederherstellungskonzepte an Ihre Risikostrategie angepasst werden?
6. Müssen Teilbereiche des Informationssicherheits- und Informationsrisikomanagements an die Krisensituation angeglichen werden?
7. Muss das IAM angepasst werden, um Ihren Mitarbeitern einen Remote-Zugriff zu ermöglichen?
8. Sind Ihre Systeme vor Überlastung geschützt und haben Sie unvorhersehbare Failover-Szenarien in Betracht gezogen?
9. Können Ihre Mitarbeiter Phishing- und Malware-Angriffe im Kontext von Covid-19 erkennen?
10. Werden Anforderungen der EU-DSGVO sowie Regelungen zur Informationssicherheit auch während der Krise eingehalten?

Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft
Ganghoferstraße 29
80339 München

Vaike Metzger
Partner, FS
T +49 89 9282-4816
vmetzger@kpmg.com

Christian Nern
Partner, FS
T +49 89 9282-6639
cnern@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia