brandeis digital

Brandeis-Check für die aktuelle Krisensituation

Krisensicheres und mobiles Arbeiten - aber kontrolliert!

Ihr Unternehmen stellt den Mitarbeitern mobile Arbeitsplätze zur Verfügung. Hardware, Lizenzen und Netzwerke wurden geprüft und ausgeliefert. Jeder Mitarbeiter wurde über eventuelle Risiken informiert und geschult. Wirklich jeder? Wie stellen Sie den störungsfreien Betrieb sicher, sollte einer Ihrer Mitarbeiter im Homeoffice Opfer einer Phishing-Attacke sein?

Haben Sie an alles gedacht?

Nutzen Sie unseren kostenfreien Service. Füllen Sie den Fragebogen aus und erfahren Sie innerhalb von 15 Minuten, wie gut Sie vorbereitet sind. Wir analysieren in allen unseren Projekten zuerst die Ist-Situation bei unseren Kunden. Wir nutzen dabei hunderte von strukturierten Fragen. Auf den folgenden Seiten finden Sie eine 50-Punkte-Checkliste, die Ihnen einen schnellen Überblick verschafft, ob und wo Sie noch nacharbeiten sollten.

Gerne stehen wir Ihnen auch mit Rat & Tat zur Seite.

Haben Sie Fragen oder wünschen Sie eine individuelle Beratung, melden Sie sich jederzeit bei uns.

Arndt Schürg
ISO/IEC 27001 Lead Auditor
+49 160 6542066

Carsten Maßloff
Geschäftsführer
+49 171 3328731

Ingo Schulenberg
Geschäftsführer
+49 170 3179024

brandeis digital

Brandeis Digital GmbH
Im Hagedorn 34
45701 Herten

E-Mail: sales@brandeis.digital
Web: www.brandeis.digital

brandeis digital

	JA	NEIN

Organisation, Rollen und Aufgaben:

1.	Ist eine Liste der Ansprechpartner für einzelne Systeme und Prozesse definiert?	☐	☐
2.	Sind Vertretungsregelungen festgelegt (z.B. Administratoren)?	☐	☐
3.	Ist definiert, wer in Rücksprache mit der Unternehmensleitung eine Krise ausrufen und krisenabhängig Vorgaben und Regeln definieren kann?	☐	☐
4.	Wurden besondere Befugnisse z.B. Weisungsbefugnisse im Krisenfall kommuniziert?	☐	☐
5.	Sind alle Kontaktdaten (Telefon, E-Mail) bekannt und auf Aktualität geprüft?	☐	☐
6.	Ist eine zentrale Stelle für die Meldung von Vorkommnissen bzw. für Fragen etabliert (z.B. Helpdesk)?	☐	☐
7.	Ist die Telefonnummer bzw. Ansprechperson zur Meldung von Vorkommnissen und Fragen allgemein bekannt? (E-Mail ist keine Alternative, da bei Systemausfall eventuell nicht mehr verfügbar), z.B. Aushang mit Namen und Telefonnummern	☐	☐
8.	Existieren Eskalationsketten bei kritischen Vorkommnissen und ist die Kommunikation an die Beteiligten sichergestellt?	☐	☐
9.	Existiert ein definiertes Krisen-Gremium mit Teilnehmern aus allen wichtigen Bereichen? Sind die Kontaktdaten aller Teilnehmer an die anderen Teilnehmer kommuniziert? Sind die Kontaktdaten aktuell?	☐	☐
10.	Ist ein durchgängiges Change-Management sichergestellt, so dass aktuelle Änderungen allen notwendigen Personen bekannt sind?	☐	☐
11.	Ist eine Kontaktperson für die Kommunikation mit Behörden benannt?	☐	☐
	Anzahl (Häufigkeit „Ja“ und „Nein“)	_____	_____

Awareness:

12.	Besitzen alle Mitarbeiter Grundkenntnisse zur Erkennung von Angriffen (z.B. Datei-Anhänge "*Dateiname.PDF.exe*")?	☐	☐
13.	Wurden die Mitarbeiter an die Einhaltung bestehender Sicherheitsvorgaben erinnert (z.B. Nutzungsvorgaben für USB-Sticks)?	☐	☐
14.	Sind Verhaltensregeln für den Krisenfall definiert und bekannt (z.B. Änderungen der Rollen und Verantwortlichkeiten, Arbeitszeitregelungen, Kommunikationsvorgaben)?	☐	☐

	JA	NEIN
15. Existieren Ausnahmeregeln zur Aufrechterhaltung des operativen Betriebs bei Ausfall von Services und Komponenten (z.B. mögliche erlaubte Nutzung privater Telefone für Gespräche aber nicht WhatsApp)?	☐	☐
16. Sind die hierfür notwendigen Informationen erfasst und für Befugte verfügbar (z.B. private Kontaktdaten wichtiger Ansprechpartner)? Sind diese Informationen vor Zugriff auf eine definierte Zielgruppe begrenzt und geschützt (DSGVO)?	☐	☐
Anzahl (Häufigkeit „Ja" und „Nein")	_____	_____

Lieferanten:

17. Existieren von Dienstleistern und Serviceanbietern Zusagen für die Aufrechterhaltung des Service im Krisenfall? Wurden Konzepte für den Ausfall von wichtigen Diensten und Lieferanten entwickelt?	☐	☐
18. Wurden für unternehmenskritische Lieferungen/ Dienstleistungen alternative Anbieter identifiziert und vertraglich gebunden?	☐	☐
19. Sind die Kontaktdaten wichtiger Ansprechpartner beim Lieferanten bekannt und dokumentiert?	☐	☐
Anzahl (Häufigkeit „Ja" und „Nein")	_____	_____

Allgemeine Risikobehandlung:

20. Sind die kritischen Systeme identifiziert und sind mögliche Sicherheitslücken analysiert (z.B. Dokumentierter Netzplan mit Clients und dazugehörigen CVE https://cve.mitre.org/)?	☐	☐
21. Sind die technisch möglichen Maßnahmen zum Schutz vor Angriffen dem aktuellen Bedrohungsszenario angemessen? Sollten Maßnahmen vorübergehend verschärft werden, auch wenn dies das Tagesgeschäft beeinflusst (z.B. Makros deaktivieren, physikalische Abtrennung kritischer Systeme im Netz)?	☐	☐
22. Ist die serverseitige Software aktuell gepatched? Sind nicht patchbare Systeme/Server dokumentiert, Gefährdungspotentiale ermittelt und notwendige Maßnahmen etabliert (z.B. vorübergehende Zugriffsbeschränkung wie Einschränkung der Administrationsrechte bei Remote- Zugriff)?	☐	☐
23. Können erweiterte Berechtigungen für Clients vorübergehend eingeschränkt (z.B. lokale Adminrechte)?	☐	☐
24. Sind Notfallhandbücher, Krisenpläne und notwendige Betriebsdokumentationen kritischer Systeme aktuell und verfügbar? Können die IT-Systeme im Notfall anhand der vorliegenden Dokumentationen wieder hochgefahren werden?	☐	☐

	JA	NEIN
25. Wurde das Wiederherstellen kritischer Daten aus dem Backup getestet?	☐	☐
26. Sind Logfiles und aussagekräftige Protokolle für eine spätere forensische Untersuchung verfügbar? Sind diese mit den Anforderungen der DSGVO abgestimmt?	☐	☐
27. Sind alle Server mit Logfiles zeitlich synchron?	☐	☐
28. Sind nicht dringend benötigte Netzzugänge eingeschränkt (z.B. Abschalten von Gast-Zugängen zur Vermeidung von Überlastungen und Angriffen)?	☐	☐
29. Wurde die Kapazität der kritischen Systeme für den Krisenfall überprüft und ausreichend ausgelegt?	☐	☐
30. Ist der VPN Zugang auf die relevante Arbeitszeit begrenzt?	☐	☐
31. Wird der Zugriff auf kritische Daten/ Informationen überwacht?	☐	☐
32. Sind die kritischen Netzwerksegmente vor unbefugtem Zugriff gesichert?	☐	☐
33. Ist eine Serverraum-Fernüberwachung möglich (Temperatur, Luftfeuchtigkeit, Kamera, Zutritt, etc.)?	☐	☐
34. Wird bei der VPN-Einwahl ein systemseitiger Compliance Check durchgeführt (Policy, Patch-Level, Status Virenscanner, etc.)?	☐	☐
Anzahl (Häufigkeit „Ja“ und „Nein“)	_____	_____

Homeoffice Risikobehandlung:

35. Ist das Betriebssystem, der Virenschutz sowie die genutzte Software auf den mobilen Endgeräten aktuell?	☐	☐
36. Sind Vorgaben zur Aufrechterhaltung der Informationssicherheit für Telearbeit einzelner Rollen definiert? Ist definiert, wie einzelne Aufgaben aufrechterhalten werden können, wenn die entsprechende Person in Quarantäne ist?	☐	☐
37. Sind die Berechtigungen für Systeme von alten Usern bereinigt (insbesondere Remote-Access)?	☐	☐
38. Sind die mobilen Endgeräte verschlüsselt?	☐	☐
39. Sind Nutzungs-Vorgaben definiert?	☐	☐
40. Wurden die Mitarbeiter auf Gefahren bei der Nutzung von Smart-Speaker im Homeoffice hingewiesen (Amazon Alexa, Apple Siri etc.)?	☐	☐
41. Wurde der Mitarbeiter, bezogen auf den Datenschutz, im Umgang mit digitalen sowie gedruckten Dokumenten hingewiesen?	☐	☐

	JA	NEIN
42. Können die mobilen Endgeräten auch extern überwacht werden?	☐	☐
43. Ist sichergestellt, dass ausschließlich Firmengeräte auf das Unternehmensnetzwerk zugreifen können?	☐	☐
44. Falls Mitarbeiter eigene Hardware verwenden, ist sichergestellt, dass diese frei von Gefahren sind (z.B. Nutzung von Citrix)?	☐	☐
45. Ist die Anbindung des Unternehmensnetzwerkes für den Krisenfall ausreichend dimensioniert (z.B. Bandbreite wegen intensiver Home-Office Nutzung)?	☐	☐
46. Werden streng vertrauliche Informationen vor externem Zugriff gesondert geschützt?	☐	☐
47. Ist das Backup für die mobilen Endgeräte im Homeoffice-betrieb sichergestellt?	☐	☐
48. Sind die Meldevorgaben bei Verlust oder Defekt der mobilen Endgeräte bekannt?	☐	☐
49. Ist der Datenverkehr zwischen Homeoffice und Firmensitz verschlüsselt bzw. ein VPN eingerichtet?	☐	☐
50. Werden Verbindungen ins Internet ohne Nutzung des VPN unterbunden?	☐	☐
Anzahl (Häufigkeit „Ja“ und „Nein“)	_____	_____

Sie haben:

- weniger als 70% der Fragen mit „Ja“ beantwortet? **Akuter Handlungsbedarf**
- zwischen 70% und 85% der Fragen mit „Ja“ beantwortet? **Kontrollierte Mitigation**
- über 85% der Fragen mit "Ja" beantwortet? **Punktuelles Nacharbeiten**