Cybersicherheits-Krisenplanung: Checkliste

Tipps für die Planung und Sicherstellung von Business Continuity mit Zscaler

zscaler™

In Zeiten der Ungewissheit ist die Gesundheit und das Wohlergehen von Mitarbeiten und Communities die oberste Priorität eines CxO. Unternehmen müssen nicht nur bei der Entwicklung sondern auch bei Betriebsabläufen agil sein, insbesondere im Katastrophenfall. Krisen können den Betrieb stören, aber die Anpassung an eine krisenbedingte „neue Normalität“ darf nicht zu Kompromissen bei der Cybersicherheit führen.

In einer Notfallsituation müssen CISOs schnell und entschlossen handeln. Zscaler identifiziert acht wesentliche strategische Ziele für CISOs in Krisenzeiten:

1. Ermöglichen und unterstützen Sie die Fernarbeit von Mitarbeitern. →
2. Ermöglichen und unterstützen Sie Sicherheitsoperationen und die Überwachung der Fernarbeit von Teams. →
3. Kalkulieren Sie erhöhte Cyberbedrohungsrisiken ein, insbesondere situationsbedingte Angriffe. →
4. Vergewissern Sie sich, dass Drittanbieter Ihre Systeme unterstützen können. →
5. Passen Sie die Prioritäten für die Unternehmenssicherheit an. →
6. Planen Sie Budgetanpassung und -kontrolle ein. →
7. Stellen Sie regulatorische Compliance sicher, selbst wenn die Einhaltung von Vorschriften erschwert ist. →
8. Beweisen Sie in einer Zeit des Wandels Führungsqualitäten. →

Jeder Krisenfall ist anders. Die folgende Checkliste soll CIOs Anhaltspunkte für das Krisenmanagement geben.

1. Ermöglichen und unterstützen Sie die Fernarbeit von Mitarbeitern.

In einer Krise – speziell bei einem Virusausbruch – müssen Mitarbeiter in der Lage sein, remote zu arbeiten. CIOs müssen folgende Überlegungen einbeziehen.

- ## Wie wird sich die Fernarbeit der Mitarbeiter auf das Rechenzentrum auswirken?
  - Das Patchen und Aktualisieren von Workflows kann ohne praktisches Eingreifen unterbrochen werden:
    - Prüfen und etablieren Sie Verfahren, um Systeme remote zu patchen und zu verwalten.
  - Die Untersuchung von Cyberverstößen und kompromittierten Geräten muss remote erfolgen:
    - Entwickeln Sie neue Prozesse für Remote-Mitarbeiter, die für Cyber-Schadensbehebung zuständig sind.
    - Erstellen Sie neue Untersuchungs- und Forensikverfahren für Remote-Mitarbeiter und Vermögenswerte.
    - Triage: Priorisieren Sie Untersuchungen und konzentrieren Sie sich zuerst auf kritische Initiativen.
  - Wenn niemand vor Ort ist, werden die drahtlosen Netzwerke des Büros zum attraktiven Angriffspunkt für Hacker:
    - Sorgen Sie dafür, dass drahtlose On-Premises-Netzwerke remote abgesichert oder bei Bedarf heruntergefahren werden können.

- ## Wird der Support für Service und Produktlizenzierung auf die Fernarbeit umgestellt?
  - Stellen Sie fest, ob sich die Anzahl der Endgerätelizenzen bei einem Anstieg der Fernarbeit ändert.
  - Stellen Sie fest, ob sich die Anzahl der Lizenzen für Cybersicherheits-Tools (einschließlich Virenschutz, Endgeräteerkennung und -reaktion, Identitätszugang und -verwaltung) bei einem Anstieg der Fernarbeit ändert.
  - Stellen Sie fest, ob der Wechsel zu BYOD-Zugang bei Fernarbeit die Lizenzanzahl beeinflusst.

- ## Wie wird sich die Umstellung eines Unternehmens auf Fernarbeit auf die Sicherheitskontrollen von Geräten auswirken?
  - Stellen Sie fest, wie sich die Fernarbeit auf Ihre Sicherheitskontrollen auswirken wird:
    - Führen Sie eine Inventur und Analyse der Kontrollen durch (verwenden Sie das NIST Cybersecurity Framework als Leitfaden).
  - Vergewissern Sie sich, dass Kontrollen remote funktionieren:
    - Im Rechenzentrum basierte Kontrollen funktionieren möglicherweise nicht mehr ohne VPN (das bei Spitzen von Remote Access überlastet sein könnte).
    - Identifizieren Sie gegebenenfalls Ausgleichskontrollen (administrative/technische).
    - Bestimmen Sie das Risiko und die Auswirkung auf DLP-Mechanismen (Data Loss Prevention).

- Stellen Sie einen Reaktionsplan für den Fall von Sichtbarkeitsverlust auf:
  - Legen Sie alternative Methoden für den Empfang von Telemetrie fest, da Sie möglicherweise nicht mehr mit Endgeräten kommunizieren können.
  - Stellen Sie die Verfügbarkeit von standardmäßigen Aktualisierungsmechanismen sicher.

Wie werden Sie die Bereinigung von Malware bewältigen?

- Richten Sie ein Verfahren zum Bereinigen von Endgeräten ein. Falls dies nicht möglich ist, stellen Sie Mitarbeitern einen Workflow für die Verarbeitung von Geräten zur Verfügung.

Wie stärken Sie eine Sicherheitskultur ohne Möglichkeit zur persönlichen Kommunikation?

- Etablieren Sie ein Verfahren zur Weitergabe von Wissen und Best Practices für Cybersicherheit.
- Fügen Sie der planmäßigen Kommunikation mit Führungskräften eine „Kurzinformation zur Sicherheit“ bei.

2. Ermöglichen und unterstützen Sie Sicherheitsoperationen und die Überwachung der Fernarbeit von Teams.

Ihre Rechenzentrums- und Sicherheitsteams arbeiten ebenfalls von Zuhause aus, während sie Mitarbeitern bei der Umstellung helfen. Dies kann Sicherheits- und IT-Workflows beeinflussen.

- Wie werden Sie mit IT-Teams im Homeoffice kommunizieren und Informationen an sie übermitteln?
  - Richten Sie E-Mail-Listen, Gruppenchats und regelmäßige (virtuelle) Meetings ein.
  - Verwenden Sie Konferenz-Tools wie Zoom oder WebEx.
  - Investieren Sie in Kollaborations-Tools wie Slack, Microsoft Teams oder Google Chat.
- Wie können IT-Teams von Zuhause aus auf Tools zugreifen und Kontrollen durchführen?
  - Modifizieren Sie die Zugangsrichtlinien, um Remote-Nutzung zu ermöglichen.
  - Verwenden Sie nach Möglichkeit Web-Frontends oder Clientanwendungen für den Remote Access.
- Wie wird sich die Reaktion auf Vorfälle ändern?
  - Erstellen Sie einen Plan zur Reaktion auf Remote-Sicherheitsvorfälle.
  - Stellen Sie einen Plan für die Behebung von Remote-Vorfällen auf.
- Wie werden Sie Identität bereitstellen/entziehen?
  - Stellen Sie sicher, dass Mitarbeitern Zugang gewährt/verweigert werden kann.
  - Reduzieren Sie gegebenenfalls Privilegien als Strategie zur Risikominderung.
  - Definieren Sie einen Plan für den Fall, dass ein SLAM-Prozess („Starters, Leavers and Movers“) die physische Anwesenheit des Mitarbeiters oder des Onboarding-Personals verlangt, einschließlich:
    - Verteilung oder Rückgewinnung von Vermögenswerten
    - Asset-Bereinigung (physisch und logisch)
    - Unterzeichnung von Dokumenten
  - Bereiten Sie sich darauf vor, Token/MFA-Mechanismen im Bedarfsfall per Post oder Paketdienst zuzustellen.

- Wie wirkt sich die Arbeit im Homeoffice auf die Sicherheitsdienste von Drittanbietern aus?
  - Bestimmen und dokumentieren Sie Zugangsbedingungen für Drittparteien.
  - Priorisieren Sie Zugangsberechtigungen für Drittparteien nach Dringlichkeit und Unmittelbarkeit.
  - Etablieren Sie einen Workflow für das Gewähren und Widerrufen von Zugangsberechtigungen für Drittparteien.

3. Kalkulieren Sie erhöhte Cyberbedrohungsrisiken ein, insbesondere situationsbedingte Angriffe.

Krisen wie der Ausbruch von COVID-19 im Jahr 2020 führen in der Regel zu einem Anstieg sogenannter „situationsbedingter“ Malware-Angriffe.

Wenn Unternehmen, die VPNs für den Remote Access verwenden, die Fernarbeit erhöhen, vergrößern sie sowohl die Distanz des MPLS-Backhauling als auch die Angriffsfläche. VPN-basierte Perimeter-Sicherheitsmodelle lassen sich bei einer Zunahme von Remote Access nicht leicht skalieren, und einige Mitarbeiter könnten versucht sein, Firewalls zu umgehen, um ins Internet zu gelangen. Hacker erkennen solche Schwachstellen und nutzen sie aus. Erschwerend kommt hinzu, dass die Übersättigung der Medien mit Kriseninformationen zu einem verminderten Sicherheitsbewusstsein führen kann: Zynische Betrüger versuchen, Malware als wichtige Krisenkommunikation zu tarnen.

Experten für Cybersicherheit (wie das Team von Zscalers eigenem ThreatLabZ) korrelieren Krisen mit der Zunahme von Datenverstößen. CISOs müssen sich mit neuen Bedrohungsrisiken befassen, die in Krisenzeiten auftauchen.

- Risikoeinschätzung: Sind Remote-Benutzer für Phishing oder andere Tricks anfällig?
  - Weisen Sie die Mitarbeiter erneut auf die Sicherheitsrichtlinien hin und informieren Sie sie über krisenbedingte Betrugsfälle.
  - Betonen Sie nachdrücklich die Bedeutung von Sicherheitssorgfalt in einer Notfallsituation.

4. Vergewissern Sie sich, dass Drittanbieter Ihre Systeme unterstützen können.

Auch Drittanbieter von Sicherheit werden ihren Betrieb an die Krisenanforderungen anpassen. Kommunizieren Sie mit Ihren Drittanbietern und verifizieren Sie, dass sich deren Support für Ihre Systeme nicht auf eine Weise ändert, die sich auf Ihre Umgebung auswirkt.

- Werden Sicherheitsanbieter Ihre an die Krise angepassten Betriebsabläufe unterstützen?
  - Überprüfen Sie den Support durch Drittanbieter:
    - Stellen Sie sicher, dass der Systemzugriff von Drittanbietern auch im Remote-Modus erhalten bleibt.
    - Überprüfen Sie das Business Continuity Planning (BCP) jedes Anbieters auf Einsatzfähigkeit und Krisendienstpläne.
    - Beachten Sie, dass insbesondere Managed Security Provider (MSSP) unter Umständen kein Potenzial für die Arbeit im Homeoffice haben. Wie können Sie dieses Risiko einkalkulieren?

5. Passen Sie die Prioritäten für die Unternehmenssicherheit an.

Bei einer Krise muss sich ein Unternehmen auf Notfallmaßnahmen konzentrieren, wobei Cybersicherheitsprioritäten möglicherweise weniger Aufmerksamkeit erhalten.

- ### Wie halten Sie die Sicherheit bei Veränderungen aufrecht?
  - Passen Sie gegebenenfalls die akzeptablen Risikostufen für Unternehmenswerte an:
    - Inventarisieren Sie physische und logische Vermögenswerte.
    - Stellen Sie sicher, dass Sie den größtmöglichen Einblick in Faktoren haben, die zum Vermögensrisiko beitragen.
    - Wägen Sie Leistung und Sicherheit ab, und passen Sie die Sicherheitslage nach Bedarf an.
  - Bewerten Sie Ihre Risikotoleranz angesichts der Umstellung auf Fernarbeit.
  - Bleiben Sie sicherheitsorientiert, ohne notwendige Änderungen oder Handlungen zu blockieren. (Sicherheit bleibt langfristig ein entscheidender Erfolgsfaktor.)

- ### Können Sie neue Prozesse, Deployments und Geräte sehen?
  - Führen Sie neue Mechanismen ein, um Reporting (Feeds, Logs, Telemetrie) remote abzurufen, zu verarbeiten und auszuwerten.
  - Etablieren Sie Verfahren, um auf diese Informationen von Systemen außerhalb des Unternehmens aus reagieren zu können.

6. Planen Sie Budgetanpassung und -kontrolle ein.

In einer Krise können Ausgaben für Notfallmaßnahmen Vorrang vor der Sicherheit erhalten. Projektfinanzierung kann gestrichen werden oder zumindest schwieriger zu beschaffen sein. Unmittelbare betriebliche Erfordernisse können den Vorzug vor Sicherheitsbelangen bekommen.

- Wird sich dies auf Ihr Betriebs- oder Planungsbudget auswirken?
  - Inventarisieren, priorisieren und klassifizieren Sie wesentliche Pläne, Geräte und Dienste.
  - Bereiten Sie sich darauf vor, Unwesentliches zu streichen (und neue Definitionen dessen, was „wesentlich“ ist, zu akzeptieren).
  - Verteilen Sie das ursprünglich für Reisen, Veranstaltungen und Zukunftsinitiativen vorgesehene Budget zur Erfüllung von Sicherheitsprioritäten um.

7. Stellen Sie regulatorische Compliance sicher, selbst wenn die Einhaltung von Vorschriften erschwert ist.

Selbst während einer Krise sind Unternehmen zur Einhaltung gesetzlicher Vorschriften verpflichtet.

- Wie werden krisenbedingte operative und strukturelle Änderungen die Fähigkeit Ihrer Organisation beeinflussen, gesetzliche Auflagen zu erfüllen?
  - Ermitteln und dokumentieren Sie, wie sich das Deployment neuer Geräte und Verfahren auf den Datenfluss und die Sicherheitsanforderungen auswirken wird.
- Werden die Notfallmaßnahmen die Fähigkeit Ihrer Organisation beeinträchtigten, Datenresidenzvorschriften zu erfüllen?
  - Stellen Sie fest, wo sich ruhende Daten befinden und wie sich Datentransferpfade ändern könnten.
  - Verifizieren Sie, dass auf neuen Datenflusspfaden Compliance gewährleistet ist. Dies könnte Korrekturen bei der Cloud- und Rechenzentrumsverwaltung und in verschiedenen geografischen Regionen sogar das Hinzufügen neuer Datenredundanz erfordern.
  - Vergewissern Sie sich, dass SSL und andere Sicherheitsmaßnahmen angewendet und geltende Datenschutzbestimmungen eingehalten werden.
- Werden Aufsichtsbehörden oder Regierungen ihre Compliance-Regeln in Krisenzeiten anpassen?
  - Verfolgen Sie behördliche Mitteilungen, die Compliance-Anforderungen betreffen.
  - Erstellen (oder zumindest planen) Sie Workflows zur Reaktion auf eventuelle krisenbedingte Anpassungen der Compliance-Anforderungen.

8. Beweisen Sie in einer Zeit des Wandels Führungsqualitäten.

Während einer Krise arbeitet jeder ohne ausreichende Informationen und muss auf eintretende Ereignisse spontan reagieren. Angesichts des Gebots, die Sicherheit zu wahren, darf ein CISO niemals aus Panik handeln. Effektive Krisenkommunikation verlangt Perspektive, Bescheidenheit, Direktheit und eine starke Stimme: Überkommunikation ohne zwingenden Grund wird zum Geräusch, Unterkommunikation dagegen erzeugt ein Informationsvakuum. Erstellen und kommunizieren Sie klare Handlungspläne.

- ### Mit wem müssen Sie kommunizieren?
  - Stellen Sie sicher, dass sich die für Sicherheit zuständigen internen Mitarbeiter über ihre Rollen, Verantwortlichkeiten, Handlungen und Verfahren im Klaren sind.
  - Vergewissern Sie sich, dass externe Interessenvertreter und Kunden über den Betrieb betreffende Änderungen informiert werden.

- ### Wie häufig müssen Sie kommunizieren?
  - Teilen Sie wichtige und unmittelbare Änderungen mit, sobald sie wirksam werden.
  - Erläutern Sie Pläne in messbaren, nachvollziehbaren Schritten mit klaren Metriken und Entwicklungsaussichten.
  - Vergewissern Sie sich, dass die Kommunikation nicht nur gesendet, sondern auch erhalten, verstanden und umgesetzt wird. Richten Sie Workflows zum Messen der Kommunikationseffizienz ein.

- ### Mit wem sollten Sie die Kommunikation koordinieren?
  - Gründen Sie ein internes Kommunikationsteam.
  - Konsultieren Sie Branchenvertreter, um Best Practices für die Kommunikation abzugleichen.
  - Erkunden Sie relevante staatliche Ressourcen (auf lokaler, länderspezifischer oder bundesstaatlicher Ebene).

- ### Wie kann ein CISO am besten eine Führungsrolle bei der Krisenkommunikation übernehmen?
  - Als Sicherheitsverantwortlicher haben Sie Erfahrung im Krisenmanagement:
    - Leiten Sie die Vorbereitungen und Notfallreaktionen Ihrer Organisation.
    - Helfen Sie den Beteiligten Ihrer Organisation bei der Einschätzung von Konsequenzen der Notfallmaßnahmen.
  - Bewahren Sie als Führungskraft Ruhe:
    - Bekämpfen Sie Angst, Ungewissheit und Panik mit Wissen, Verständnis und Vorbereitung.

Die in der Cloud entwickelte Secure Access Service Edge Platform von Zscaler ist speziell dafür konzipiert, direkte Konnektivität über lokale Internet-Breakouts zu ermöglichen, damit Unternehmen (und ihre sämtlichen Remote-Mitarbeiter) auch in ungewissen Zeiten vorankommen können.

Zscalers Business Continuity Program unterstützt Organisationen dabei, selbst unter schwierigsten Bedingungen ihre erstklassige Sicherheitslage beizubehalten.

Mehr erfahren

Über Zscaler

Zscaler wurde im Jahr 2008 auf der Grundlage eines einfachen aber wirkungsvollen Konzepts gegründet: Da Anwendungen in die Cloud verlagert werden, muss sich auch die Sicherheit dorthin bewegen. Heute helfen wir Tausenden von globalen Organisationen bei der Transformation zu Cloud-fähigen Betriebsabläufen.