Top-kritische Risiken für die Identitätssicherheit

von PATECCO

KI-gestütztes Phishing

❑ Das Risiko

- ✓ KI ermöglicht äußerst überzeugendes Phishing, Identitätsdiebstahl und Kompromittierung von Geschäfts-E-Mails
- ✓ Generative und agentenbasierte KI macht gefälschte Nachrichten praktisch identisch mit echten.
- ✓ Multimodale KI (Text + Sprache + Video) ermöglicht groß angelegte, gezielte Angriffe
- ✓ Stimmenklonung kann Führungskräfte imitieren und für Betrugsversuche missbraucht werden

❑ Auswirkung

- ✓ Erhöhtes Risiko von Kontokompromittierung und Betrug
- ✓ Erhebliche finanzielle Verluste und Reputationsschäden

❑ Maßnahmen zur Risikominderung

- ✓ Multi-Faktor-Authentifizierung (MFA) durchsetzen
- ✓ Identitätsprüfungs- und Anti-Phishing-Tools verwenden
- ✓ Verhaltensbasierte Bedrohungserkennung implementieren

Automatisierte Malware

❑ Das Risiko

- ✓ Angreifer nutzen Automatisierung, um Schwachstellen sofort zu scannen
- ✓ Exploits und Malware werden schneller als je zuvor generiert und eingesetzt
- ✓ Zero-Day-Schwachstellen werden innerhalb weniger Stunden als Waffen eingesetzt

❑ Auswirkung

- ✓ Minimierung der Patch-Bereitstellungszeit
- ✓ Höheres Risiko einer raschen Systemkompromittierung

❑ Maßnahmen zur Risikominderung

- ✓ Automatisiertes Patch-Management implementieren
- ✓ Endpoint Detection & Response (EDR) einsetzen
- ✓ Echtzeit-Überwachung mit Bedrohungsinformationen nutzen
- ✓ Manuelle Reaktionsverzögerungen reduzieren

Identitäts- und Zugriffsangriffe

- ❑ **Das Risiko**
  - ✓ Diebstahl von Zugangsdaten und Session-Hijacking nehmen zu
  - ✓ Synthetische Identitäten sind schwerer zu erkennen
  - ✓ MFA-Fatigue-Angriffe umgehen herkömmliche Authentifizierung
- ❑ **Auswirkung**
  - ✓ Account-Übernahme
  - ✓ Laterale Bewegung innerhalb von Netzwerken
- ❑ **Maßnahmen zur Risikominderung**
  - ✓ Zero-Trust-Architektur einführen
  - ✓ Privilegiertes Zugriffsmanagement (PAM) stärken
  - ✓ Phishing-resistente Authentifizierungsmethoden verwenden
  - ✓ Identitätsaktivitäten kontinuierlich überwachen

Cloud- und API-Exposition

❑ Das Risiko

- ✓ Falsch konfigurierte Cloud-Umgebungen legen sensible Daten offen.
- ✓ Privilegienverlagerungen nehmen mit der Zeit zu.
- ✓ Exponierte APIs dienen Angreifern als Einstiegspunkt

❑ Auswirkung

- ✓ Unbefugter Zugriff auf sensible Daten und kritische Systeme.
- ✓ Höheres Risiko für Datenlecks, Ausfälle und weitreichende Sicherheitsvorfälle

❑ Maßnahmen zur Risikominderung

- ✓ Strenge IAM-Richtlinien durchsetzen
- ✓ Regelmäßige Konfigurationsprüfungen durchführen
- ✓ API-Zugriff kontinuierlich überwachen

Ransomware

❑ Das Risiko

- ✓ KI-gesteuertes Targeting macht Ransomware-Angriffe präziser und effektiver
- ✓ Fortgeschrittene Taktiken kombinieren Verschlüsselung, Datendiebstahl und Drohungen mit öffentlicher Veröffentlichung
- ✓ Angriffe zielen zunehmend darauf ab, Geschäftsabläufe zu stören, nicht nur Zahlungen zu erzwingen

❑ Auswirkung

- ✓ Finanzielle Verluste
- ✓ Reputationsschaden
- ✓ Betriebsausfall

❑ Maßnahmen zur Risikominderung

- ✓ Sichere Offline-Backups pflegen
- ✓ Netzwerke und sensible Daten segmentieren
- ✓ Strenge Zugriffskontrollen anwenden

Insider-Risiken & menschliche Fehler

❑ **Das Risiko**

✓ Unbeabsichtigte Fehler von Mitarbeitenden
✓ Fehlkonfigurationen in komplexen hybriden Umgebungen
✓ Datenlecks durch überlastete Teams

❑ **Auswirkung**

✓ Datenexposition
✓ Privilegienmissbrauch
✓ Interne Sicherheitsverletzungen

❑ **Maßnahmen zur Risikominderung**

✓ Least-Privilege-Zugriff erzwingen
✓ Privilegiertes Zugriffsmanagement (PAM) implementieren
✓ Sessions und verdächtige Aktivitäten überwachen

Datenschutz und Compliance-Lücken

❑ Das Risiko

- ✓ Neue Vorschriften erhöhen die Compliance-Anforderungen
- ✓ Unzureichende Prüfpfade und unverwaltete Endpunkte schaffen Risiken
- ✓ Schwache Kontrolle des Fernzugriffs führt zu Verstößen

❑ Auswirkung

- ✓ Regulatorische Bußgelder und Strafen
- ✓ Zunehmende Verluste durch Sicherheitsverletzungen
- ✓ Reputationsschäden

❑ Maßnahmen zur Risikominderung

- ✓ Starke Protokollierungs- und Audit-Kontrollen implementieren
- ✓ Sichere Workflows für den Fernzugriff gewährleisten
- ✓ Cybersicherheitsstrategie an regulatorische Standards anpassen

Kontaktieren Sie uns. Wir unterstützen Sie gerne!

PATECCO GmbH
+49 (0) 23 23 - 9 87 97 96
www.patecco.com
info@patecco.com