www.itbusiness.ch Fractal Verlag GmbH Ausgabe 4/2024 CHF 10.–

itbusiness

Das Schweizer Fachmagazin für ICT

KI-Potenziale in ERP-Systemen nutzen

Nachhaltige IT – unterschätzte Einsparpotenziale

Cybersicherheit 2025: Strategien gegen neue digitale Gefahren

Cybersecurity 2025: Strategien für eine neue Ära digitaler Bedrohungen

Cybersecurity ist heute weit mehr als nur eine technische Herausforderung – sie steht im Zentrum der strategischen Agenda vieler Unternehmen. Die digitale Transformation bringt tiefgreifende Veränderungen in Arbeitsprozessen, Technologien und Geschäftsmodellen mit sich, und Cyberkriminelle entwickeln parallel dazu immer raffiniertere Angriffstechniken.

Michael Ghezzo

Wie kann sich die Unternehmenswelt diesen Entwicklungen anpassen? Beim Gartner Symposium in Barcelona, einem der bedeutendsten Branchentreffen für CIOs und IT-Entscheider, gaben Analysten entscheidende Einblicke in die Trends und Herausforderungen, die das Thema Cybersicherheit in den nächsten Jahren prägen werden.

Drei Schlüsselanforderungen an die Cybersecurity-Führung von morgen

Für die kommenden Jahre kristallisieren sich drei zentrale Anforderungen heraus, denen sich Chief Information Security Officers (CISOs) stellen müssen, um auf die veränderten Sicherheitsanforderungen angemessen zu reagieren:

1. **Transformation des Digital Operating Models**
   Die traditionelle Rolle der Cybersecurity als «Blocker» von Projekten ist längst nicht mehr zeitgemäss. Gartner geht davon aus, dass bis 2027 über 75 Prozent der Mitarbeitenden Technologien selbstständig erwerben, verändern oder entwickeln werden – ohne formale IT-Beteiligung. Dieser Trend zur sogenannten «Schatten-IT», deren Anteil 2022 bereits 41 Prozent erreichte, führt zu erheblichen Sicherheitslücken und zwingt CISOs, die Rolle der IT-Sicherheit neu zu definieren und dezentraler zu gestalten.

2. **KI als strategisches Element in der Cybersecurity**
   Künstliche Intelligenz (KI) entwickelt sich rasant und verändert auch die Spielregeln der Cybersecurity. Um die wachsenden Herausforderungen zu meistern, müssen CISOs die Rolle der KI in vier Bereichen verstehen und gestalten:

   - Defend with AI: Immer mehr Sicherheitstools setzen auf KI, doch sind nicht alle Lösungen ausgereift. Datenschutzfragen und Wirksamkeit stehen hier noch zur Debatte.
   - Attacked by AI: Angreifer nutzen zunehmend KI für gezieltere und effektivere Attacken.
   - Build und Consume AI: KI bietet potenziell zahlreiche Anwendungen, bringt aber auch Risiken mit sich – insbesondere hinsichtlich geistigen Eigentums und Datenschutzes. Die unkontrollierte Nutzung von «Schatten-KI» erhöht die Angriffsfläche zusätzlich.

3. **Ein menschenzentriertes Sicherheitskonzept**
   In einer Unternehmenswelt, in der Fachbereiche ihre IT-Initiativen zunehmend unabhängig vorantreiben, kann eine sichere Cybersecurity nur durch Zusammenarbeit und eine menschenzentrierte Sicherheitsarchitektur erreicht werden. Gartner empfiehlt daher, Cybersecurity stärker auf die Bedürfnisse und Verhaltensweisen der Mitarbeitenden abzu-

stimmen und alle Mitarbeitenden aktiv in das Sicherheitsmanagement einzubinden.

Acht entscheidende Prognosen für die Cybersecurity der Zukunft

Neben den unmittelbaren Anforderungen an das Security-Management zeichnet Gartner in seinen Vorhersagen ein präzises Bild davon, welche Veränderungen die Cybersecurity in den kommenden Jahren prägen werden. Acht Prognosen geben dabei einen Einblick, was Unternehmen erwarten können und welche Massnahmen strategisch sinnvoll sind:

1. **Managerhaftung in der Cybersecurity erweitern**
   Bis 2027 werden zwei Drittel der Top-100-Unternehmen ihre D&O-Policen (Versicherungen gegen Managerhaftung) auch auf Führungskräfte im Bereich Cybersecurity ausweiten. Angesichts steigender Bedrohungen und verschärfter Regulierungsanforderungen soll dies das Risiko der Kriminalisierung und die potenzielle finanzielle Belastung von CISOs minimieren.

2. **Kampf gegen Desinformation und Fake News intensivieren**
   Laut Gartner werden Unternehmen bis 2028 weltweit 500 Milliarden Dollar gegen Desinformation und Fake News aufwenden – das wird die Hälfte der Budgets für Cybersecurity und Marketing beanspruchen. AI-gestützte Social-Engineering-Techniken, Deepfake-Betrug und Angriffe auf den Ruf von Unternehmen und Führungskräften erfordern erhebliche Investitionen.

3. **Generative KI schliesst die Qualifikationslücke**
   Generative KI (GenAI) wird die Qualifikationslücke im Bereich Cybersicherheit bis 2028 teilweise schliessen. KI-basierte Tools für Routineaufgaben werden die Anforderungen an Einstiegspersonal reduzieren und eröffnen neue Chancen für Quereinsteiger.

4. **Zero-Trust-Konzepte anpassen**
   Gartner schätzt, dass bis 2026 etwa 75 Prozent der Unternehmen ungemanagte Systeme, Legacy-Systeme und OT (Operational Technology) aus ihren Zero-Trust-Sicherheitsmodellen ausschliessen müssen. Die Lücke zwischen modernen digitalen Plattformen und älteren Technologien wird sich damit weiter vertiefen.

5. **Reduktion der durch Mitarbeitende verursachten Cybervorfälle**
   Die Kombination aus GenAI, integrierten Plattform-Architekturen und einem verbesserten Nutzerverhalten wird bis 2026 zu einer Verringerung von Cybervorfällen durch Mitarbeitende um 40 Prozent führen. Dies unterstreicht die Bedeutung einer Aufklärungskampagne, die das Sicherheitsbewusstsein der Belegschaft stärkt.

6. **Neue Rolle des Identity- und Access Managements**
   Ab 2026 werden Verantwortliche für Identity- und Access Management (IAM) auch für die Reaktion auf IAM-bezogene Security-Vorfälle zuständig sein. Die wachsende Bedeutung digitaler Identitäten verlangt nach einer stärkeren Integration von IAM in die Gesamtstrategie der Cybersecurity.

7. **Zusammenwachsen von Data Loss Prevention, Insider Risk Management und IAM**
   Bis 2027 werden diese Disziplinen enger vernetzt sein. Die steigende Bedrohungslage im Bereich Insider-Risiken und Datenverluste macht ein umfassendes Identitätsmanagement notwendig, um den steigenden Anforderungen gerecht zu werden.

8. **Sicherheitsverantwortung für Applikationen in die Applikationsteams verlagern**
   Die zunehmende Nutzung von No- und Low-Code-Plattformen erfordert, dass die Verantwortung für die Sicherheit von Applikationen zunehmend in die Applikationsteams verlagert wird. Schulungen und neue Standards werden notwendig sein, damit Entwickler Sicherheitsfragen direkt in ihre Arbeit integrieren.

Neue Wege für eine sichere Zukunft

Die Trends und Prognosen der Analysten verdeutlichen die tiefgreifenden Veränderungen, die die Zukunft der Cybersecurity prägen werden. Die zunehmende Dezentralisierung der IT, die steigende Bedeutung von KI und die Rolle des Menschen im Sicherheitsprozess machen deutlich, dass Cybersecurity mehr denn je eine strategische Priorität ist. Führungskräfte im Bereich Cybersecurity müssen ihre Ansätze anpassen und einen klaren Fokus auf innovative Lösungen legen, um den komplexen Herausforderungen der digitalen Zukunft gerecht zu werden. www.confare.at ■