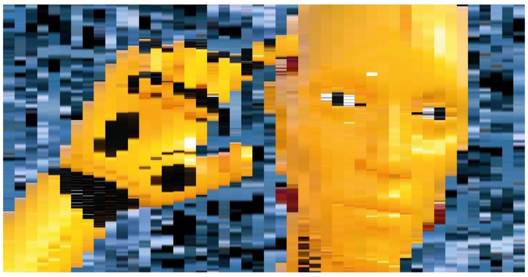
KI NOCH NICHT REIF FÜR CYBERSECURITY



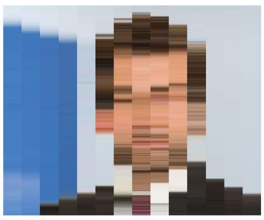
Wenn es um den Einsatz im Security-Bereich geht, hat KI noch viel zu lernen.

Im Wesentlichen sind es zwei große Hindernisse, die dem flächendeckenden Einsatz von KI in der Cybersicherheit im Wege stehen. Die liegen zum einen in unzureichend ausgereiften KI-basierten Technologien selbst und zum anderen im Zeit- und Ressourcenmangel der betreffenden Abteilungen und Unternehmen begründet. Das hat eine Umfrage von BlackBerry Cylance in Zusammenarbeit mit dem SANS Institute ergeben. Wenn die Implementierung von künstlicher Intelligenz in die Cybersecurity jedoch sachgerecht vonstatten geht, dann bietet KI eine Reihe von Vorteilen. |CB

MEHR ALS DIE HÄLFTE DER UNTERNEHMEN TESTEN IHRE NOTFALLPLÄNE NICHT

Eine IBM-Ponemon Studie zur Resilienz gegen Cyberangriffe zeigt, dass eine große Mehrheit der Unternehmen noch immer nicht darauf vorbereitet ist, angemessen auf Cyberangriffe zu reagieren. 77 Prozent der Unternehmen haben demnach keinen einheitlichen, unternehmensweiten Notfallplan. »Wenn es darum geht, auf einen Cyberangriff zu reagieren, ist fehlende Planung der erste Schritt zum Misserfolg. Die Notfallpläne müssen daher regelmäßig auf Herz und Nieren geprüft werden«, sagt Ted Julian, Mitgründer von IBM Resilient. |CB

ISPA: »REGIERUNG PLANT TOTALÜBERWACHUNG«



»Die Bundesregierung hebelt unter dem Vorwand, eine Digitalsteuer einzuführen, um sogenannte Internetgiganten stärker zu besteuern, die Grundrechte der Bürger aus. Sie schafft gigantische Datensilos für Werbefirmen und ebnet gleichzeitig der Totalüberwachung und der Bespitzelung der österreichischen Bevölkerung den Weg. Der Entwurf zum Digitalsteuergesetz 2020 ist als Totalüberwachungsgesetz zu bezeichnen und schlichtweg desaströs« so ISPA Generalsekretär Maximilian Schubert. |CB

GASTKOMMENTAR | DER UMGANG DES TOPMANAGEMENTS MIT CYBERKRISEN

Frequenz, Komplexität und Intensität von Cyberangriffen verzeichnen einen starken Anstieg. Nicht ohne Grund gilt Cyberkriminalität als eine der Top 5-Unternehmensrisiken, so das World Economic Forum in seinem »Global Risks Report 2019«. Dies ist jedem IT-Experten klar. Aber ist das auch den Geschäftsführern und Vorständen bewusst? Mit anderen Worten: Ist das letztverantwortliche Topmanagement auf Cyberkrisen vorbereitet?

Keine Sympathie für angegriffene Unternehmen

Nach einem Cybervorfall liegt das größte Schadenspotenzial für eine Organisation nicht in technischen Aufräumarbeiten, sondern im drohenden Imageschaden. Denn es gibt keine Sympathie (mehr) für gehackte Unternehmen. Alle Stakeholdergruppen weisen mittlerweile eine kritische Sensibilität gegenüber digitalen Attacken auf. Egal, ob Endkunde, Lieferant oder Behörde, sie alle wollen von der betroffenen Unternehmensführung genau wissen, welche Auswirkungen die Cyberattacke auf sie haben könnte. Für die Schadensminimierung ist also entscheidend, wie eine Organisation einen derartigen Vorfall kommuniziert.

Reputationsschaden durch Vorkehrungen abwenden

Wir als Berater sehen auf der Führungsebene ein steigendes Problembewusstsein für das Reputationsrisiko – und das ist gut so. Für die Unternehmensspitze ist es wichtig, sich der Tragweite digitaler Risiken bewusst zu werden und entsprechende organisatorische sowie kommunikative Vorkehrungen zu treffen. Ist ein Datenleck einmal entdeckt, sind Ausmaß, Dauer und Tiefe des Angriffs noch lange nicht klar. Diese andauernde Unsicherheit stellt für die Kommunikation eine große Herausforderung dar. Außerdem sind unerwartete Entwicklungen oder auch Medienanfragen zu erwarten, die eine rasche Bewertung und eine angemessene Reaktion erfordern. Um entsprechend (re-)agieren zu können, ist ein schlankes, koordiniertes und flexibles Krisenteam notwendig, das sich mit der Unternehmensspitze abstimmt. Beharrliches Schweigen als Reaktion würde hingegen die Unternehmensreputation nachhaltig schädigen und Kunden sowie andere relevante Stakeholder verschrecken.

ALEXANDER KLEEDORFER | BRUNSWICK GROUP

GOOGLE WILL IM CLOUD-GESCHÄFT AUFHOLEN

Google Cloud hat die allgemeine Verfügbarkeit von Anthos verkündet, einer Plattform, auf der Kunden Anwendungen vor Ort, in der Google Cloud, aber vor allem mit anderen großen Public Cloud-Anbietern wie Microsoft Azure und Amazon Web Services (AWS) ausführen können. Kunden sollen damit die Möglichkeit haben, ihre Anwendungen zu nutzen, wo immer sie wollen und reibungslos Daten hin- und herzuschieben. Anthos ist eine Software-Lösung, die auf Googles Kubernetes-Engine setzt. »Cloud ist eine der größten Investmentbereiche des Unternehmens«, so Google-Chef Sundar Pichai. |CB