Nachgefragt

ICT-Sicherheit zu gewährleisten zählt zu einer der wichtigsten Aufgaben für Unternehmen. Wir fragten bei ICT-Sicherheits-Profis nach Schwachstellen und Bedrohungsszenarien nach.

Thomas Meier
CEO
InfoGuard AG
www.infoguard.ch

Welche Angriffsarten stellen Sie in diesem Jahr häufiger fest?
Die Anzahl und die Professionalität jeglicher Angriffsarten nimmt zu. Auffallend oft finden Spearphishing-Attacken statt. Angreifer nutzen heutzutage selbst die kleinsten Schwachstellen in IT-Systemen aus. Unternehmen sind gefordert, ihre Systeme ausreichend zu schützen. Ein grosses Risiko stellt zudem der Mensch dar. Ungenügende Awareness der Mitarbeitenden oder eine Missachtung der Sicherheitsvorgaben können fatale Folgen haben.

Welches sind, aus Ihrer Erfahrung heraus typische Schäden, die Unternehmen in Folge eines Cyberangriffes zu erwarten haben?
Der offensichtlichste Schaden ist sicher der finanzielle. Aber auch die Wiederherstellung des Betriebes und der Systeme ist kostspielig. Nicht zu vergessen sind die Reputationsschäden.

Auf welche zukünftigen Bedrohungsszenarien müssen sich Unternehmen besonders einstellen?
Unternehmen müssen sich bewusst sein, dass sie früher oder später angegriffen werden – oder bereits infiltriert sind. Die Erkennung, Analyse und Abwehr von Cyberattacken ist daher essentiell. Cyber Defence muss fester Bestandteil jeder Cyber Security-Strategie sein.

Der Trend geht ausserdem hin zu Cloud-Lösungen, die jedoch grosse Sicherheitsrisiken bergen. Einfluss auf die Bedrohungslage haben aber auch politische und wirtschaftliche Entwicklungen, die Treiber für gezielte Attacken sein können. Das sind nur einige Bedrohungsszenarien, auf die sich Unternehmen in Zukunft gefasst machen müssen.

Steve Mayer
Country Manager
Citrix Schweiz
www.citrix.com

Welche Netzwerkinfrastrukturen beinhalten die grössten Sicherheitsrisiken in den Unternehmen?
Netzwerke, die vor dem Internet-Zeitalter aufgesetzt wurden und sukzessive erweitert wurden, entwickelten mit der Zeit isoliert operierende Bereiche. Die individuellen Schwachstellen erleichtern Hackern den Zugriff, zudem sind sie durch unterschiedliche Sicherheitslösungen aufwändiger zu überwachen.

Welches sind die wichtigsten Massnahmen zum Schutz der Netzwerkinfrastruktur?
Eine zentral verwaltete Infrastruktur mit übergreifenden Lösungen, die das Unternehmen als Ganzes erfassen, inklusive sämtlicher Endgeräte wie Handys oder Laptops. Diese verringern den administrativen Aufwand und schaffen ganzheitliche Transparenz. Starke Authentifizierungsmassnahmen mit kontextbasiertem Zugriff und nutzerdefinierten Rechten schränken Hacker zusätzlich ein.

Auf welche zukünftigen Bedrohungsszenarien müssen sich Unternehmen besonders einstellen?
Ransomware hat sich als lukratives Mittel für Hacker erwiesen. Diese Methode wird künftig noch verfeinert werden. So war WannaCry im vergangenen Jahr schon eine Weiterentwicklung, die wurmartige Eigenschaften der Verbreitung aufwies und somit ein Novum darstellte.