IT-Sicherheit von morgen

Prognose zu Cybersecurity-Trends 2024

München im November 2023. Digitalisierung, Authentifizierung und Remote Work sind längst für sämtliche Unternehmen Realität. Mit einem hohen Preis: 148 Milliarden Euro Schaden entsteht der deutschen Wirtschaft jährlich durch Cyberangriffe. Nach einer Bitkom-Studie waren bereits 84 % aller deutschen Unternehmen betroffen. Ein Zeichen für die Dringlichkeit, sich der IT-Sicherheit zu widmen. Worauf sollten Firmen beim Wappnen gegen Bedrohungen achten? Welche Trends sind im Bereich Informationstechnik relevant und im kommenden Jahr zu erwarten? Diese Fragen klärt Yakup Saygin, IT-Sicherheits-Experte und Gründer der Münchner Entwicklerfirma Saytec.

Arbeiten von überall

Remote Work verkörpert heutzutage eine feste Arbeitsform und einen fundamentalen Teil vieler Berufe. Laut einer Umfrage vom Leibniz-Zentrum für Europäische Wirtschaftsforschung erlauben 80 % der teilnehmenden Informationswirtschaftsfirmen ihren Beschäftigten, mindestens einmal pro Woche im Home Office zu arbeiten. Doch was mit Vorteilen wie dem fehlenden Arbeitsweg, flexibleren Zeiten und einer ausgewogenen Work-Life-Balance lockt, birgt auch einige Nachteile. Allein durch Unwissenheit öffnen Internetnutzer Eingangstore für Hacker und Schadsoftware. Private Geräte, private Netzwerke oder herkömmliche Cloud-Lösungen vergrößern die Problematik.

Das Internet der Dinge

Das Netz breitet sich aus – Smart Speaker, Smart Watches, Sensoren oder intelligente Kühlschränke tragen als Bestandteile des Internet of Things zur zunehmenden Alltagsdigitalisierung bei. Statista zufolge fahren spätestens bis zum Jahr 2030 10 % aller Autos autonom. Die Zukunft verspricht eine intelligente Kommunikation zwischen allen Geräten, die auch den Menschen, etwa durch Smart Watches, Brillen oder Kleidung, mit einbindet. Diese Vernetzung, auch Internet of Everything genannt, winkt mit Boni wie Zeitersparnis durch schnellere technische Entscheidungen oder Problemlösungen. Werden Bestandteile des Netzes wie Sensoren oder selbstfahrende Autos jedoch als Sicherheitslücke unterschätzt und unzureichend vor Angriffen geschützt, drohen Personenschäden, Produktdefizite, Manipulation oder Datendiebstahl.

Intelligente Computer

Künstliche Intelligenz ist im Unternehmenskontext angekommen. Laut der Bitkom stieg die gewerbliche Nutzung von KI-Systemen im letzten Jahr von 9 auf 15 % an, 64 % aller Unternehmen sehen KI als essenzielle Zukunftstechnologie. In der Zeitspanne zwischen den Jahren 2023 und 2030 soll der KI-Markt jährlich um 37,3 % wachsen. Bis zum Jahr 2030 steigt das Bruttoinlandsprodukt nur durch den KI-Markt um 11,3 %. In der IT-Security nützt Künstliche Intelligenz beim frühzeitigen Erkennen ungewöhnlicher Aktivitäten und Angriffe, der Durchforstung von Hackerforen und der Analyse von Dark Web Marktplätzen. Auf der anderen Seite sorgt sie durch Identitätsdiebstahl oder Deepfakes für Glaubwürdigkeit von Phishing-Mails. Schadprogramme wie sogenannte Ransomware schränken folgend den Zugriff auf Daten oder Programme ein. Für die Freigabe fordern die Erpresser häufig hohe Lösegelder, wobei eine Bezahlung die Rückgabe digitaler Schätze nicht garantiert.

Pressekontakt: Borgmeier PR Hamburg
Hanna Reschke, Claudia Bendrat | 040 / 413096-14, -10 | reschke@borgmeier.de, bendrat@borgmeier.de

Vertrauen ist gut, Zero Trust ist besser

Authentifikation ist der Schlüssel – die Zero-Trust-Strategie vertraut keinem Gerät, Nutzer oder Netzwerk vor ihrer Verifizierung. Das System bewertet jede Zugriffsanfrage, zieht anschließend entsprechende Schlüsse, gewährt oder verweigert den Zugriff beziehungsweise fordert eine zusätzliche Authentifizierung. Kontext spielt ebenfalls eine große Rolle: Eine eindeutige Identitätsprüfung des Anwenders verhindert Missbrauch durch Identitätsklau. Single Sign-on eignet sich zur Absicherung kritischer Anwendungen und Systeme, ohne umständlich mit unterschiedlichen Passwörtern umzugehen. Zero Trust stellt jedem Anwender nur ganz bestimmte Programme und Daten zur Verfügung, die dessen Authentifizierung erfordern. Während einer Sitzung werden Gerät und Nutzer kontinuierlich überprüft. Laut Gartner werden bis 2025 60 % aller Unternehmen eine Zero Trust Strategie etablieren. Die Strategie bietet Schutz, permanente Überwachung und stellt besonders für Firmen, die auf Cloud-Lösungen und Remote Work setzen, eine Entlastung dar.

Open Source Software

70 % aller befragten Unternehmen setzen Open Source Software ein – das ergab die Bitkom-Studie „Open Source Monitor 2023“. Offene Programme kosten oft weniger und punkten gegenüber Closed Source Programmen mit Flexibilität. Hinzu kommt ein öffentlich abrufbarer Quellcode, den User nach Belieben verändern können. Da Millionen Augen mehr sehen als zwei, merzen aufmerksame Nutzer Fehler schnell aus. Erkannte Sicherheitslücken finden ihren Weg ins Internet und warnen Open-Source-Verbündete im Handumdrehen.

Über Saytec

Die Saytec AG mit Sitz in München wurde 2015 von Physiker Yakup Saygin gegründet. Das IT-Unternehmen setzt sich zum Ziel, jeden Computer branchenübergreifend von jedem Ort aus und installationsfrei vor IT-Risiken zu schützen. Zu diesem Zweck entwickelte Saytec SAYTRUST VPSC (Virtual Private Secure Communication). Die personifizierte Zero-Trust-Technologie bietet achtstufigen Schutz sowohl remote als auch aus dem Firmennetzwerk: Anwendende checkt sie zentral im Arbeitsspeicher, bevor sie Unternehmensanwendungen nutzen und das Netzwerk betreten. Damit schließt sie eine maßgebliche Sicherheitslücke. Der technologische Ansatz und die zentrale Handhabung beenden die Abhängigkeit von Endgeräten und damit auch von Sicherheitslücken auf Endgeräten. All-in-one-System SAYFUSE vervollständigt das Security-Portfolio: Die skalierbare, modular einsetzbare IT-Infrastruktur-Komplettlösung mit Backup-Plattform und Hochsicherheitscloud dient Sammlung, Schutz, Erhalt und Verfügbarkeit der Unternehmenswerte und vereinfacht die vorhandene IT-Komplexität um bis zu 70 Prozent. Selim Kuzu führt die Geschäfte des Security-Unternehmens, das die Vision antreibt, IT-Sicherheit für jeden erschwinglich zu machen. Mehr Informationen liefert www.saytec.eu

Pressekontakt: Borgmeier PR Hamburg
Hanna Reschke, Claudia Bendrat | 040 / 413096-14, -10 | reschke@borgmeier.de, bendrat@borgmeier.de