Bitkom e.V. | Presseinformation

IT-Sicherheit: Was Unternehmen jetzt dringend tun sollten

- **Der Krieg in der Ukraine wird auch im digitalen Raum geführt**
- **Unternehmen sollten Schutzmaßnahmen nachziehen, klare Verantwortlichkeiten festlegen und die Mitarbeitenden sensibilisieren**

Berlin, 04. März 2022 - Die russische Offensive begann im digitalen Raum bereits einige Zeit vor dem Einmarsch in die Ukraine. „Während Cyberangriffe auf militärische Zielsysteme, Behörden und Institutionen bereits seit längerem stattfinden, spielte der digitale Raum in den ersten Tagen des russischen Angriffskriegs nur eine nachgelagerte Rolle. Mit zunehmender Kriegsdauer könnte sich dies wieder ändern, und das kann unmittelbare Konsequenzen für Deutschland und seine Wirtschaft haben. Denn die Distanzen im digitalen Raum sind kurz und die Grenzen nicht so klar, wie sie sein müssten“, erklärt Bitkom-Sicherheitsexperte Sebastian Artz. „Es gibt keinen Grund zur Panik, aber mit dem Angriffskrieg Russlands ist auch im deutschen Cyberraum volle Aufmerksamkeit und größtmögliche Wachsamkeit aller Unternehmen, Organisationen und staatlichen Stellen geboten.“

Der Digitalverband Bitkom gibt fünf konkrete Hinweise, welche Vorbereitungen und Vorsichtsmaßnahmen insbesondere kleine und mittelständische Unternehmen jetzt treffen sollten:

1. Risiken und Auswirkungen von Cyberangriffen minimieren

Unternehmen sollten ihre Schutzmaßnahmen insgesamt verstärken. Betriebssysteme und Software müssen auf dem aktuellen Stand sein, Sicherheitsupdates sind zügig einzuspielen. Sichere – also komplexe und für jedes System unterschiedliche – Passwörter tragen signifikant zur Erhöhung des Schutzniveaus bei. Möglichst alle Logins mit Außenanbindung sollten über eine Multi-Faktor-Authentifizierung geschützt werden. Privilegien und Administrationsrechte sollten für einzelne Nutzerinnen und Nutzer eingeschränkt werden und die Komplexität von verwendeten Diensten insgesamt verringert werden. Eine solche Härtung der Systeme ist trotz Einschränkung der Nutzungsfreundlichkeit und Produktivität zum Schutz der eigenen Infrastruktur und unternehmenssensiblen Daten ratsam. Zudem ist die unternehmenseigene Backup-Strategie zu prüfen und nachzuziehen, sodass alle relevanten Unternehmensdaten gesichert sind und zusätzlich Sicherheitskopien offline auf einem externen Datenträger existieren.

2. Verantwortlichkeiten klar definieren

Unternehmen müssen in einem Angriffsfall reaktionsfähig sein. Es braucht die klare Definition von Verantwortlichkeiten im Sicherheitsbereich und die Einrichtung entsprechender Anlaufstellen – sowohl intern als auch bei externen Dienstleistern. Es gilt sicherzustellen, dass zu jeder Zeit ausreichend Personal einsatzfähig ist. Urlaubszeiten oder Vertretungen bei Krankheit müssen dabei einkalkuliert werden. Außerdem ist es sinnvoll sich darauf vorzubereiten, auch ohne die Hilfe externer Dienstleister kurzfristig reagieren zu können – bei großflächigen Cyberangriffen könnten Externe an Kapazitätsgrenzen stoßen.

3. Beschäftigte sensibilisieren

Alle Erfahrungen zeigen: Der Mensch bleibt eines der größten Sicherheitsrisiken, ist aber auch Schutzgarant eines Unternehmens. Alle Beschäftigten sollten zielgruppengerecht für das erhöhte Risiko von Cyberangriffen sensibilisiert werden. Dazu gehört, potenzielle Gefahren verständlich zu erklären und Schritt-für-Schritt-Anleitungen bereitzustellen, wie man sich im Falle eines Angriffs verhält und an wen man sich wenden muss. Gegebenenfalls können kurzfristige Sicherheitsschulungen sinnvoll sein. Ziel ist es, die Wachsamkeit in der Belegschaft zu erhöhen. Besonders für den E-Mail-Verkehr gilt, Hyperlinks und Anhänge nicht vorschnell zu öffnen und

ungewöhnliche Anweisungen mit Skepsis zu betrachten. An Unternehmen werden auch sehr gezielte und gut gemachte Phishing-Mails geschickt, wodurch der Fake nur anhand weniger Details wie etwa eines falsch geschriebenen Namens oder einer falschen Durchwahl in der Signatur entdeckt werden kann.

4. Notfallplan erstellen

Für den Fall eines Angriffs sollte im Unternehmen ein Notfallplan bereitliegen, der das weitere Vorgehen dokumentiert. Neben den technischen Schritten, die eingeleitet werden müssen, sollte der Plan auch organisatorische Punkte wie die Kontaktdaten relevanter Ansprechpersonen im Unternehmen sowie die Notfallkontakte der offiziellen Anlaufstellen beinhalten. Auch rechtliche Aspekte wie Meldepflichten bei Datenschutzverletzungen müssen berücksichtigt werden. Des Weiteren gehört eine vorbereitete Krisenkommunikation dazu, um schnell alle relevanten Stakeholder wie Kundinnen und Kunden, Partnerinnen und Partner sowie die Öffentlichkeit zu informieren.

5. Informationen offizieller Stellen beobachten

Die Sicherheitslage ist hochdynamisch und kann sich von Tag zu Tag ändern. Unternehmen sollten daher die Meldungen von Behörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie der Allianz für Cybersicherheit (ACS) stets beobachten. Aktuelle Informationen finden Sie hier:

- https://www.bsi.bund.de
- https://www.allianz-fuer-cybersicherheit.de

Weitere Informationen zu den Auswirkungen des Krieges auf die digitale Welt gibt es hier: https://www.bitkom.org/Ukraine

Kontakt

Andreas Streim
Pressesprecher
Telefon: +49 30 27576-112
E-Mail: a.streim@bitkom.org

Felix Kuhlenkamp
Bereichsleiter Sicherheitspolitik
Nachricht senden

Link zur Presseinformation auf der Webseite:
https://www.bitkom.org/Presse/Presseinformation/IT-Sicherheit-Was-Unternehmen-jetzt-dringend-tun-sollten