NACHRICHTEN AG

26. August 2024

Straubinger Unternehmen Opfer eines digitalen Ransomware-Angriffs

In Straubing wurde ein Unternehmen Opfer eines Ransomware-Angriffs. Daten könnten betroffen sein. Polizei ermittelt.

In der Nacht vom 19. auf den 20. August wurde ein Unternehmen im Straubinger Stadtgebiet schwer von einem Cyberangriff betroffen. Gegen 9 Uhr bemerkten Mitarbeiter, dass die Firmencomputer durch sogenannte Ransomware mutwillig blockiert und unbrauchbar gemacht wurden. Besonders alarmierend ist, dass es bislang keine Kontaktaufnahme durch die unbekannten Täter gegeben hat, wodurch die Situation noch rätselhafter bleibt.

Das betroffene Unternehmen meldete den Vorfall umgehend der Polizei. Schnell wurde ein sogenanntes Quick-Reaction-Team der Kriminalpolizeiinspektion Straubing aktiviert, welches bereits mit der Untersuchung des Angriffs begonnen hat. Die Firma versucht nun, mit Unterstützung ihres IT-Dienstleisters, auf bestehende Datensicherungen zuzugreifen, um den regulären Betrieb wiederherzustellen. Bislang ist jedoch unklar, ob sensible Daten eventuell entwichen sind. Der durch den Ausfall verursachte Schaden wird vorläufig auf einen niedrigen fünfstelligen Eurobetrag geschätzt.

Ransomware – Ein Überblick

Ransomware ist ein besonders gefährlicher Typ von Schadsoftware, die Rechner oder Dateien des Opfers verschlüsselt, sodass der Nutzer keinen Zugriff mehr auf seine

Daten hat. Die Täter verlangen häufig ein „Lösegeld“, oft in Kryptowährungen, um die Entschlüsselung wieder freizugeben. Experten raten dringend davon ab, das geforderte Geld zu zahlen, da es keine Garantie gibt, dass die entschlüsselten Daten auch tatsächlich wiederhergestellt werden können und der Druck auf die Betroffenen unter Umständen nur weiter steigt.

- Aktualisieren Sie Ihre Software und Betriebssysteme regelmäßig, um Sicherheitslücken zu schließen.
- Verwenden Sie stets aktuelle Antiviren-Software.
- Erstellen Sie regelmäßig Backups wichtiger Daten auf externen Speichermedien.
- Im Schadensfall können Sie kostenfreie Entschlüsselungstools auf der Website www.NoMoreRansom.org finden, die in Zusammenarbeit mit Europol und anderen Partnern entwickelt wurden.
- Seien Sie vorsichtig mit E-Mail-Anhängen von unbekannten Absendern.

Wichtige Sicherheitsmaßnahmen für Unternehmen

Um sich vor digitalen Angriffen wie diesen zu schützen, sollten Unternehmen präventive Schritte unternehmen. Eine der besten Maßnahmen ist die Strukturierung der Netzwerkinfrastruktur, was bedeutet, dass verschiedene Teile des Netzwerks voneinander getrennt werden, um das Risiko einer Ausbreitung von Malware zu minimieren. Zudem spielt der Zugang zu Netzen und Computern eine entscheidende Rolle – Zugriffsrechte sollten so gestaltet sein, dass nur autorisierte und notwendige Personen Zugang haben.

- Beschränken Sie die Zugriffsrechte Ihrer Mitarbeiter und definieren Sie klar, welche Softwareprodukte verwendet werden dürfen.
- Schulen Sie Ihre Mitarbeiter regelmäßig zu den Risiken und möglichen Angriffsszenarien, und stellen Sie

Verhaltensregeln auf.

Das Bundesamt für Sicherheit in der Informationstechnik bietet zahlreiche Ressourcen und Informationen, die Unternehmen und Privatpersonen dabei helfen können, sich vor den wachsenden Bedrohungen im digitalen Raum zu schützen. Die Prävention und Bildung über Ransomware und deren Gefahren sind entscheidend für den Schutz sensibler Daten.

Cybersecurity im Fokus

Dieser Vorfall zeigt eindrücklich, wie wichtig Cybersicherheit in der heutigen Zeit ist. Alle Unternehmen – unabhängig von ihrer Größe – sollten sich der Gefahren bewusst sein, die von digitalen Angriffen ausgehen. Präventive Maßnahmen und der verantwortungsvolle Umgang mit sensiblen Daten sind unerlässlich, um schwere finanzielle Verluste und den Verlust von wertvollen Informationen zu vermeiden. Ransomware stellt eine ernsthafte Bedrohung dar, die nicht nur auf technische Maßnahmen angewiesen ist, sondern auch auf das Bewusstsein und die Wachsamkeit der Mitarbeiter.

Ransomware-Angriffe sind nicht nur ein aktuelles Problem, sondern haben sich über die letzten Jahre zu einer ernsthaften Bedrohung für Unternehmen aller Größenordnungen entwickelt. Die Zunahme solcher Angriffe ist eng verbunden mit der digitalen Transformation vieler Firmen, die ihre Prozesse und Daten zunehmend online verlagern. Laut einer Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI) wurden im Jahr 2022 über 1500 Attacken gemeldet, was einen Anstieg von 30 % im Vergleich zum Vorjahr bedeutet. Diese Bedrohungen betreffen nicht nur die Technik, sondern können auch tiefgreifende Auswirkungen auf die wirtschaftliche Stabilität von Unternehmen haben.

Einfluss auf die Unternehmenssicherheit

Die Auswirkungen eines Ransomware-Angriffs sind oft

verheerend. Neben direkten finanziellen Schäden, die durch Betriebsausfälle und Lösegeldforderungen entstehen, gibt es auch langfristige Konsequenzen wie Vertrauensverlust bei Kunden und Partnern sowie mögliche rechtliche Schritte, insbesondere wenn personenbezogene Daten betroffen sind. Eine Umfrage des Digitalverbands Bitkom hat gezeigt, dass fast jedes zweite Unternehmen (46 %) in Deutschland zuletzt keine ausreichenden Maßnahmen zum Schutz vor Cyberangriffen ergriffen hat.

Die Rolle von IT-Sicherheitsschulungen

Um Unternehmen vor solchen Bedrohungen zu schützen, wird die Schulung der Mitarbeiter immer entscheidender. Die Menschen sind oft das schwächste Glied in der Sicherheitskette. Phishing-E-Mails, die häufig als Aufhänger für Ransomware-Angriffe dienen, können durch grundlegende Schulungen und Sensibilisierung der Mitarbeiter effektiver abgewehrt werden. Unternehmen sollten mindestens einmal jährlich verpflichtende Schulungen zur IT-Sicherheit durchführen, um sicherzustellen, dass ihre Mitarbeiter gegen aktuelle Bedrohungen gewappnet sind.

Statistiken zur Cyberkriminalität

Jahr	Angriffe	Verluste in Millionen Euro
2020	1200	128
2021	1150	144
2022	1500	200

Diese Zahlen verdeutlichen den kontinuierlichen Anstieg von Ransomware-Angriffen und den damit verbundenen finanziellen Schäden. Unternehmen sollten sich nicht nur auf technische Lösungen verlassen, sondern auch ihre gesamte Unternehmenskultur in Richtung Sicherheit und Risikomanagement anpassen.

Aktuelle Entwicklungen im Bereich der Cybersecurity

Die Reaktion auf die steigende Zahl von Ransomware-Angriffen hat auch zu einem Anstieg an Kooperationen zwischen staatlichen Stellen und Unternehmen geführt. Projekte wie **No More Ransom** sind ein Beispiel dafür, wie private und öffentliche Organisationen zusammenarbeiten, um Betroffenen zu helfen und die Verbreitung von Ransomware einzudämmen. Behörden wie Europol und nationale Sicherheitsagenturen stellen Tools und Ressourcen zur Verfügung, um Unternehmen bei der Wiederherstellung ihrer Systeme zu unterstützen und präventive Maßnahmen zu fördern.

Zusätzlich hat die Bundesregierung Schritte unternommen, um Unternehmen zu ermutigen, ihre Sicherheitsinfrastruktur zu verbessern. Diese Bemühungen werden durch Förderprogramme und Initiativen zur Aufklärung über Cybersecurity unterstützt, um Unternehmen in Deutschland sicherer zu machen. Die Diskussion über Cybersecurity wird somit zu einem zentralen Thema in der unternehmerischen Strategie und der nationalen Sicherheitsagenda.

Details