Top 10 Notfall-Tipps bei einem Ransomware-Angriff

1. **Trennung des betroffenen Bereichs**: Unmittelbar nach Erkennung eines Ransomware-Befalls sollten Sie die infizierten Systeme sofort von der restlichen Netzwerkumgebung abkoppeln. Dies beinhaltet die physische Trennung vom Netz sowie das Deaktivieren jeglicher drahtlosen Verbindungen wie Wi-Fi und Bluetooth.
2. **Erhebung und Protokollierung der Vorfälle**: Halten Sie präzise fest, welche Bereiche, Daten und Services kompromittiert wurden. Protokollieren Sie sorgfältig alle ergriffenen Maßnahmen und registrierten Unregelmäßigkeiten, da diese Informationen für die Aufarbeitung des Vorfalls und eventuelle juristische Nachspiele von Bedeutung sind.
3. **Meldung an zuständige Stellen und Geschäftspartner**: Informieren Sie sofort die verantwortlichen Sicherheitsinstitutionen und eventuell betroffene Geschäftspartner über den Vorfall, besonders wenn Risiken für deren Systeme bestehen.
4. **Interne Kommunikationsmaßnahmen**: Unterweisen Sie Ihre Belegschaft umgehend über den Sicherheitsvorfall und instruieren Sie sie über vorläufig zu treffende Sicherheitsmaßnahmen wie den Verzicht auf Zugriffe auf bestimmte Systemteile oder das Melden suspekter E-Mails.
5. **Einbeziehung von Cybersicherheitsexperten**: Holen Sie IT-Sicherheitsfachleute oder spezialisierte Beratungsfirmen an Bord, um die Malware zu begutachten und einen Plan für die Säuberung sowie die Systemwiederherstellung auszuarbeiten. Prüfen Sie Möglichkeiten der professionellen Datenwiederherstellung bei Ransomware.
6. **Überprüfung der Datensicherungen**: Kontrollieren Sie Ihre Datenbackups hinsichtlich ihrer Unversehrtheit und Autonomie vom Hauptnetzwerk. Bestätigen Sie, dass die Backups nicht von der Ransomware betroffen sind, bevor Sie mit einer Wiederherstellung fortfahren.
7. **Beratung bezüglich des Lösegelds**: Konsultieren Sie mit Fachleuten und behördlichen Stellen über die Zweckmäßigkeit einer Lösegeldzahlung. Oft wird von einer Zahlung abgeraten, da diese keine sichere Rückgewinnung der Daten verspricht und potenziell weitere Angriffe anregt.
8. **Planung der Wiederinbetriebnahme**: Erarbeiten Sie einen präzisen Plan für die Reinigung und Wiederinbetriebnahme der beeinträchtigten Systeme, in enger Kooperation mit Sicherheitsexperten.
9. **Beseitigung der Sicherheitsdefizite**: Ermitteln Sie die Einfallspforte der Ransomware und treffen Sie Maßnahmen, um die identifizierten Sicherheitsmängel zu beheben. Aktualisieren Sie Ihre Sicherheitsprotokolle und führen Sie Schulungen für Ihre Belegschaft durch, um das Sicherheitsbewusstsein zu schärfen.
10. **Überprüfung und Optimierung der Sicherheitsstrategien**: Nachdem der Zwischenfall behoben wurde, sollten Sie Ihre Sicherheitsstrategien gründlich überdenken und anpassen, um zukünftigen Angriffen besser vorzubeugen. Dazu zählen regelmäßige Überprüfungen der Sicherheitsmaßnahmen, die Aktualisierung der Sicherheitstechnologien und kontinuierliche Mitarbeiterschulungen.