Schutz vor digitaler Erpressung

Abwehrstrategien zum Schutz vor Lösegeldforderungen, Schadensersatzansprüchen und Imageschäden

Ransomware (Erpressungssoftware) gehört zu den gefährlichsten Arten von Schadsoftware, ist extrem verbreitet und hat sich zu einer der **größten Bedrohungen für die digitale Welt** entwickelt. Für betroffene Unternehmen stellt Ransomware eine **existentielle Bedrohung** dar.

Was ist Ransomware?

Diese von Hackern genutzten **Schadprogramme** greifen auf Computersysteme zu und **blockieren/verschlüsseln** sie so, dass der Benutzer nicht mehr darauf zugreifen kann. Durch Zahlung eines hohen **Lösegeldes** (z.B. über eine Kryptowährung wie Bitcoins), erhält man die Möglichkeit, die Daten mit einem einzigartigen Schlüssel zu entschlüsseln. Zahlt man zu spät oder gar nicht, erfolgt die Löschung des Schlüssels, alle Daten sind dann unwiderruflich verschlüsselt und für immer verloren. In vielen Fällen erfolgen aber nach einer Zahlung des Lösegeldes **weitere Forderungen** anstatt des versprochenen Schlüssels.

Wie gelangt Ransomware auf ein Computersystem?

Meist gelangen Ransomware-Trojaner über **(Phishing-)eMails** in ein Computersystem. Klickt man einen darin enthaltenen Link an, wird das System infiziert. Eine Infektion ist aber auch über **Webseiten**, die Schadprogramme enthalten, möglich.

Wie schützt man sich vor Ransomware?

Ransomware wird weiterhin eine maßgebliche Bedrohung sein. Deshalb gilt es, sich entsprechend vor einer möglichen Attacke zu schützen:

Konsequentes Patch Management (Systemaktualisierungen)
Halten Sie Ihren Antiviren-Schutz, jegliche Software und das Betriebssystem stets aktuell - am besten automatisiert.

Administratorenrechte verwalten
Die Installationsprivilegien sollten bei den IT Mitarbeitern und/oder dem betreuenden IT Systemhaus liegen. Dadurch wird verhindert, dass Endbenutzer schädliche Software installieren.

Blue Shield Umbrella
Diese bereits mehrfach ausgezeichnete IT Security Lösung sorgt dafür, dass Gefahren nicht nur erkannt, sondern präventiv geblockt werden. Lesen Sie mehr über Blue Shield Umbrella auf www.deutsche-systemhaus.eu/flexible-loesungen/blue-shield-umbrella.

Makros, Plug-ins
Deaktivieren Sie die automatische Makro-Ausführung, grenzen Sie die Verwendung von Browser-Plug-ins weitestgehend ein.

Mitarbeiterschulungen und Richtlinien
Klären Sie Ihre Mitarbeiter über Angriffsflächen und den richtigen Umgang mit eMails und Webseiten auf. Klare Richtlinien zur Nutzung der IT Systeme erhöhen ebenfalls die Sicherheit.

Last but not least: BACKUP – BACKUP – BACKUP
Sollte es trotz aller Vorsichtsmaßnahmen zu einem Angriff kommen, können Sie durch eine konstante Datensicherung Ihre Daten wiederherstellen. Voraussetzung ist ein optimales Sicherungskonzept, das alle Faktoren miteinbezieht, wie z.B. Rotation, Verschlüsselung, Automatisierung, Aufbewahrung an verschiedenen Orten, regelmäßige Restore-Tests, etc.

Sie möchten die IT Sicherheit Ihres Unternehmens erhöhen? Wir beraten und unterstützen Sie gerne dabei, die Gefahr von Cyberangriffen zu minimieren.

09431 7173 130
marketing@d-s.group
www.deutsche-systemhaus.eu

Deutsche Systemhaus

facebook.com/ds.deutsche.systemhaus
twitter.com/DS_Systemhaus