HORNETSECURITY

INFO SHEET

RANSOMWARE

WIE UNTERNEHMEN SICH EFFEKTIV SCHÜTZEN KÖNNEN

Ransomware gilt als die größte Cyber-Bedrohung für Unternehmen weltweit (Quelle: World Economic Forum, 2025). Kriminelle setzen dabei verstärkt auf hochentwickelte, automatisierte Angriffsketten, die mithilfe von generativer KI-Technologie immer ausgefeilter werden. Besonders perfide: Viele Angriffe starten mit scheinbar harmlosen E-Mails – und enden in der Verschlüsselung ganzer Systeme. Eine Umfrage von Hornetsecurity zeigt: Jedes dritte Unternehmen war 2024 von Datenverlust aufgrund von Ransomware betroffen.

WAS IST RANSOMWARE?

Ransomware (auch Verschlüsselungstrojaner oder Erpressungstrojaner) ist eine Schadsoftware, die Computer oder Dateien verschlüsselt und den Zugriff darauf blockiert, bis ein Lösegeld (engl. „ransom“) gezahlt wird. Sie wird meist unbemerkt installiert und tritt anschließend direkt mit dem Opfer in Kontakt. Ransomware ist besonders gefährlich, da sich die Schadsoftware in Netzwerken verbreiten kann und so ganze Organisationen lahmlegt.

MÖGLICHE ANGRIFFSVEKTOREN:

Phishing-Angriffe: Oft reicht ein einziger Klick auf einen schädlichen Link oder eine Antwort auf eine manipulierte E-Mail aus, um den Angriff zu starten.

E-Mail & -Anhänge: Ransomware wird häufig über infizierte Office-Dokumente, ZIP-Dateien oder PDFs verbreitet. Gerade E-Mails mit personalisiertem Inhalt sind schwer zu erkennen und entgehen herkömmlichen Filtern leicht.

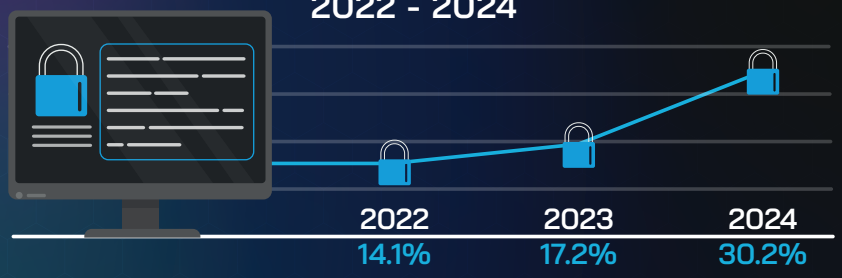
Schwache Zugangsdaten: Einfach zu erratende Passwörter oder fehlende Multi-Faktor-Authentifizierung erleichtern Angreifern den Zugriff auf Systeme.

Ungepatchte Systeme: Ungepatchte Systeme: Angreifer nutzen bekannte Schwachstellen in Software und Systemen aus. Lückenhaftes Patchen ist daher ein gefundenes Fressen für Ransomware.

Social Engineering-Taktiken: Social Engineering-Taktiken: Mitarbeiter werden gezielt manipuliert, z.B. durch Anrufe oder gezielte Support-Anfragen. Täter setzen hierbei oft auf Stress, Autorität oder Dringlichkeit, um zu unüberlegten Handlungen zu verleiten.

HORNETSECURITY

OPFER VON RANSOMWARE-ANGRIFFEN MIT DATENVERLUSTEN 2022 - 2024



SCHUTZSTRATEGIEN GEGEN RANSOMWARE:

SCHÄDLICHE E-MAILS ZUVERLÄSSIG BLOCKIEREN	SPAM & MALWARE PROTECTION	Phishing E-Mails sind nach wie vor einer der häufigsten Einfallstore für Ransomware. Sicherheitslösungen wie Spam and Malware Protection blockieren schädliche Anhänge und infizierte Links, bevor Schaden angerichtet wird.
MODERNE BEDROHUNGEN FRÜHZEITIG ERKENNEN	ADVANCED THREAT PROTECTION	Ransomware wird zunehmend ausgeklügelter. Eine Schutzmaßnahme auf Basis von selbstlernender KI kann auch versteckte oder neuartige Bedrohungen erkennen und abwehren – nutzen Sie beispielsweise Advanced Threat Protection.
KRITISCHE SCHWACHSTELLEN IM BLICK BEHALTEN		Angreifer nutzen häufig bekannte Sicherheitslücken in Software oder veralteten Systemen aus, um Ransomware einzuschleusen. Halten Sie Ihre Systeme daher permanent aktuell, idealerweise mit einem zentralisierten Patch-Management, und nutzen Sie überall wo möglich eine Mehrfaktor-Authentifizierung (MFA).
MITARBEITER AKTIV EINBINDEN	SECURITY AWARENESS	Die beste Technik nützt nichts, wenn das menschliche Verhalten zur Schwachstelle wird. Sensibilisieren Sie Ihre Teams durch regelmäßige Schulungen und simulierte Phishing-Kampagnen mit Security Awareness Service – und fördern Sie eine nachhaltige Sicherheitskultur in Ihrem Unternehmen.
DATEN IM ERNSTFALL SCHNELL WIEDERHERSTELLEN	VM BACKUP 365 TOTAL BACKUP	Trotz aller Prävention ist Schutz nie zu 100 % garantiert. Umso wichtiger ist es, die Daten zu schützen. Mit VM Backup V9 und 365 Total Backup können Sie Ihre Backups in der gesicherten Infrastruktur von Hornetsecurity speichern. So sind die Daten vor Ransomware-Angriffen geschützt.