ensec INFORMATION SECURITY

RANSOMWARE

Lassen Sie sich nicht erpressen

Ransomware-Attacken haben in den letzten Jahren stark zugenommen. Betroffen sind neben Privatpersonen Firmen aller Branchen und Grössen. Das Vorgehen der Erpresser wird dabei immer perfider.

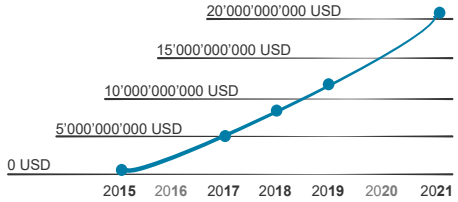
Das Aufkommen von Cryptoblocker, Cryptowall und anderer Ransomware mit ähnlich guter Verschlüsselung, führte um das Jahr 2014 zu einem wahren Boom der digitalen Erpressung. Dass auch heute noch Unternehmen mit dieser Methode erpresst werden, liegt am Erfolg, den die Erpresser in vielen Fällen haben.

Was ist Ransomware? Unter dem Begriff werden unterschiedliche Arten von Schadprogrammen zusammengefasst, die den Zugriff auf Daten oder Systeme blockieren, um damit das Opfer zu erpressen. Die bekanntesten ihrer Art verwenden dazu starke Verschlüsselung und versprechen die Herausgabe des notwendigen Schlüssels gegen Bezahlung eines Lösegelds (meist in Form von Bitcoin).

Gemäss dem US Department of Justice fanden 2016 täglich mehr als 4000 derartige Angriffe statt. Die üblichen Erpressungssummen belaufen sich auf 200 – 5000 USD. Jedoch wurden auch bereits wesentlich höhere Summen erpresst. So bezahlte etwa das «Hollywood Presbyterian Hospital» 17'000 USD Lösegeld – verlangt hatten die Hacker zuvor einen Millionenbetrag. Falls, wie in diesem Fall, am Ende den Forderungen nachgegeben wird, stellen die Lösegeldzahlungen meist einen vergleichsweise kleinen Teil der gesamten Schadensumme dar. Oft viel grösser sind die Schäden welche durch Prozess- oder Betriebsunterbrechungen entstehen.

Auch Schweizer Unternehmen sind betroffen. In den Medien ist fast jeden Monat ein Bericht zu einem Schweizer Unternehmen zu lesen, welches Opfer einer Ransomware-Attacke wurde. Wobei davon auszugehen ist, dass bloss die wenigsten Fälle publik werden. Während einige mit einem blauen Auge davon kommen, trifft es andere so schwer, dass sie in den Konkurs getrieben werden.

Weltweite Schäden durch Ransomware
Source: Cybersecurity Ventures



Die Bedrohung nimmt weiter zu. Verschiedene Studien zeigen, dass Ransomware-Attacken über die vergangenen paar Jahre stetig zugenommen haben. Und Experten gehen davon aus, dass in den kommenden Jahren mit einem weiteren Anstieg zu rechnen ist. Ein Trend der vermutlich noch lange anhalten wird, da sich immer wieder attraktive Opfer finden und die Erpresser durchaus gewillt sind ihre Taktiken anzupassen – so wird seit einiger Zeit auch mit der Veröffentlichung gestohlener Daten gedroht.

47.1388422
72.9917328

Wie können sich Unternehmen schützen?

An dieser Stelle gilt es zu betonen, dass keine einzelne Massnahme oder Sicherheitslösung existiert, die Ihr Unternehmen umfassend vor Ransomware schützt. Vielmehr geht es darum kontextbezogen in Prävention, Detektion und Reaktion zu investieren um die Verwundbarkeit zu minimieren und die Resilienz zu erhöhen. Eine solide Endpoint-Security-Lösung, Offline-Backups, wirkungsvolle Sensibilisierung der User und eine Stärkung der Netzwerksicherheit bilden dazu die Basis.

Endpoint Security Die Absicherung der Endgeräte durch eine moderne und aktuelle Sicherheits-Suite, hilft bei der frühzeitigen Entdeckung von Schad-software und kann deren Ausführung im Idealfall verhindern.

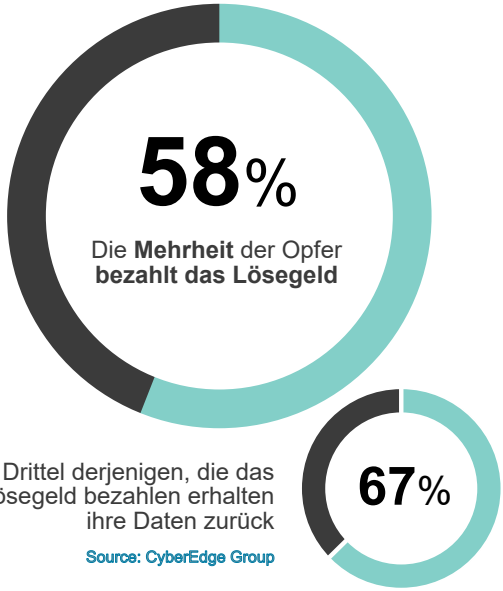
Offline Backups Da moderne Ransomware auch Backups angreift, sind Offlinekopien oft die einzige Möglichkeit verlorene oder verschlüsselte Daten wiederherzustellen.

User Awareness Der einfachste und nach wie vor häufigste Weg auf welchem Ransomware in ein Firmennetzwerk gelangt, sind schlecht informierte und unvorbereitete Nutzer. Mit geschickt konzipierten und adäquat durchgeführten Schulungen und Präventionskampagnen, lässt sich dieses Risiko nachweislich senken.

Netzwerksicherheit Durch eine passende Segmentierung des internen Netzwerkes, lässt sich die Verbreitung von Schadsoftware effektiv eindämmen und besonders wichtige Daten und Systeme besser schützen. Zusätzlich sorgen moderne Firwalls für einen optimierten Schutz des Perimeters.

Daneben sollten **Software-Schwachstellen zeitnah behoben werden**, da solche von Ransomware direkt ausgenutzt werden.

Unternehmen die darüber hinaus weitere Sicherheitsmassnahmen in Betracht ziehen wollen, sind gut beraten, sich über die Themen Web-Isolierung, Content-Security, System-härtung (Hardening) und “Security Information and Event Management” (SIEM) zu informieren. All diese Konzepte können einen erweiterten Schutz vor Schadsoftware aller Art bieten.



ensec unterstützt Sie und ist Ihr Partner für sämtliche Information Security Fragen - natürlich auch im Bereich Ransomware-Schutz.

Mit der langjährigen Erfahrung ihrer Experten, verfügt ensec über das notwendige Know-how und kann Ihr Unternehmen von der Strategie-definition bis zur Umsetzung der passenden Massnahmen mit Beratung und Integrations-dienstleistungen unterstützen.

Wichtig sind Lösungen welche sowohl die menschlichen und organisatorischen Aspekete, als auch die technischen Komponenten gleichermassen berücksichtigen. Dies ist im Kampf gegen Ransomware besonders wichtig, da unvorsichtige und/oder ungeschulte Nutzer das Einfallstor Nummer 1 für Schadstoff-software darstellen.