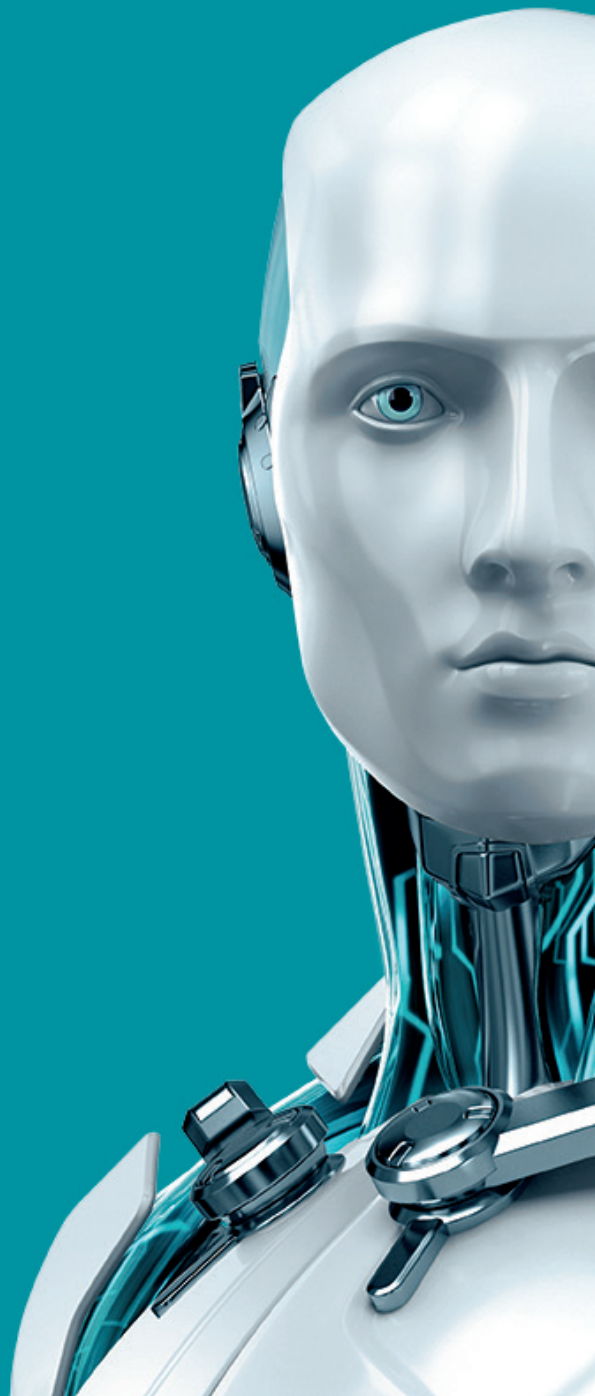
ENJOY SAFER TECHNOLOGY™

RANSOMWARE

Wie Sie Ihr Unternehmen vor erpresserischer Malware schützen



Inhalt

2 Vor Ransomware schützen

4 Schützen Sie Ihre Unternehmens-Rechner

7 Was tun, wenn mein Rechner bereits infiziert ist?

8 Behalten Sie auch die Android-Geräte im Blick

9 Was tun, wenn mein Android-Gerät bereits infiziert ist?

10 Zu guter Letzt: Soll ich das Lösegeld bezahlen?

Zusammenfassung

Bei Ransomware, auch Erpressungs- oder Verschlüsselungstrojaner genannt, handelt es sich um Schadsoftware, die den Zugriff auf Geräte sperrt oder darauf enthaltene Daten verschlüsselt und anschließend vom Opfer ein Lösegeld für die Wiederherstellung verlangt. Diese Schädlinge können mit einem Zeitschalter ausgestattet sein, um den Nutzer zusätzlich unter Druck zu setzen. Nach Ablauf der vorgegebenen Zeit kann so das zu zahlende Lösegeld erneut erhöht oder der Zugriff auf die Daten unwiderruflich gesperrt werden.

Für Desktop-Computer zählen Reveton, CryptoLocker, CryptoWall und TeslaCrypt zu den bekanntesten Beispielen für diese Form von Erpresser-Software; auf mobilen Plattformen haben Simplocker und LockerPin schon Tausende an Android-Geräten infiziert.

ESET-Analysen zufolge wird Ransomware unter Cyberkriminellen immer populärer und in den letzten Jahren für Angriffe gegen Unternehmen und Privatanwender vermehrt eingesetzt. Selbst wenn Windows und Android zu den am häufigsten betroffenen Betriebssystemen gehören, belegen aktuelle Vorfälle, dass Ransomware auch vor Linux und OS X nicht Halt macht.

Dieses Whitepaper zeigt häufig genutzte Angriffsvektoren auf und bietet einen Leitfaden zum Schutz Ihrer Systeme und Daten im Unternehmen. Durch die aufgeführten Handlungsoptionen im Falle eines Ransomware-Angriffs lassen sich die eventuelle Folgen um ein Vielfaches begrenzen.

Zuletzt beantwortet ESET die wichtigste aller Fragen von Ransomware-Opfern: Soll ich das von den Cyberkriminellen geforderte Lösegeld bezahlen?

Vor Ransomware schützen

Insbesondere für Unternehmen steht viel auf dem Spiel. Verlieren sie den Zugriff auf wichtige Unternehmensressourcen, kann der finanzielle Schaden und Imageverlust enorm hoch ausfallen. Eine aktuelle *Umfrage* unter knapp 3.000 IT- und Cybersicherheits-Experten weltweit zeigt, dass mindestens eins von fünf Unternehmen bereits dieser Gefahr ausgesetzt war.

Angreifer nutzen heutzutage genauso starke Verschlüsselungen wie z.B. Banken zum Schutz des Zahlungsverkehrs ihrer Kunden einsetzen. Diese starke Verschlüsselungsmethode erschwert die Wiederherstellung von Geräten oder Dateien – im schlimmsten Fall ist sie sogar unmöglich.

Es lohnt sich also auch aus finanziellen Gründen, in Präventivmaßnahmen zu investieren. Sind die Vorkehrungen zum Schutz der Unternehmensdaten nur unzureichend und Mitarbeiter ungenügend sensibilisiert, besteht ein deutlich erhöhtes Risiko für einen Ransomware-Befall und den damit verbundenen Verlust von Zeit und wertvoller Daten.

A. Verwenden Sie stets die aktuellste Programmversion ihrer Sicherheitslösung

Nutzen Sie immer die aktuellste Programmversion Ihres Sicherheitssoftware-Anbieters. Viele Schädlinge schaffen es vor allem aufgrund veralteter Lösungen, das System zu befallen. Bei ESET können Sie, bei Besitz einer gültigen Lizenz, jederzeit auf die neueste Programmverision updaten.

Ältere ESET Endpoint Security Produkte der Versionen 3 oder 4 können Sie nicht vor moderner Ransomware schützen. Wir empfehlen dringend den Einsatz unserer aktuellen Version 6 des Business-Produkts. Sie enthält die neuesten Technologien mit verbessertem Client-Schutz und wehrt selbst verschlüsselte oder getarnte Malware zuverlässig ab.

Darunter gehören unter anderem die **Erweiterte Speicherprüfung**, die Malware blockiert, sobald sie ihre schädlichen Funktionen erkennen lässt sowie der **Exploit Blocker**, der zielgerichtete Angriffe auf bisher unbekannte Schwachstellen, auch Zero-Day-Exploits genannt, verhindert.

B. Achten Sie auf die Aktualität der Virensignaturdatenbank

Immer wieder werden neue Ransomware-Versionen verbreitet. Umso wichtiger ist es, dass die Virensignaturdatenbank von allen Computern und anderen Firmengeräten stets auf dem neuesten Stand ist. Dies verbessert den Schutz vor Ransomware und anderen Schädlingen. ESET Security-Produkte aktualisieren stündlich die Virensignaturdatenbank, sofern sie über eine gültige Lizenz verfügen und mit dem Internet verbunden sind.

Aktivieren Sie das ESET LiveGrid® Cloudsystem

Unbekannte und potenziell schädliche Anwendungen sowie andere mögliche Bedrohungen werden beobachtet und über das ESET Live Grid® Feedback-System an die ESET Cloud übermittelt. Hier werden die gesammelten Samples in einer Sandbox einer umfassenden Analyse unterzogen. Erkennt ESET eine Bedrohung und stuft sie als schädlich ein, wird für alle Anwender eine Erkennungssignatur erstellt.

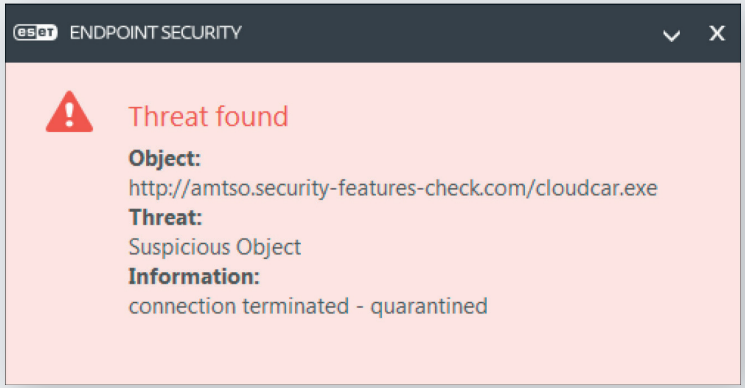
Sie wird unseren Kunden sofort und unabhängig vom nächsten Update der Signaturdatenbank über das ESET LiveGrid® Reputationssystem zur Verfügung gestellt. Auch als unsicher eingestufte Vorgänge – z.B. das Löschen eines Backups – werden umgehend gestoppt. Um den Schutz Ihrer Privatsphäre zu gewährleisten nutzt ESET LiveGrid® lediglich die Hashes verdächtiger Dateien, das heißt, es werden keinerlei Inhalte übertragen.

WICHTIGER HINWEIS

In manchen Fällen wird die ESET LiveGrid Kommunikation durch Ihre Unternehmens-Firewall blockiert. Testen Sie, ob diese Funktion ordnungsgemäß funktioniert. Mehr Informationen dazu finden Sie auf der Webseite der Non-Profit-Prüforganisation AMTSO, bei der auch ESET Mitglied ist:

http://www.amtso.org/feature-settings-check-cloud-lookups/

Klicken Sie auf den Link „Download the CloudCar Testfile" und laden Sie die Testdatei „cloudcar.exe" herunter. Funktioniert ESET LiveGrid ordnungsgemäß, wird die Datei vom ESET LiveGrid® System erkannt und auf ihrem System sofort blockiert. Im Anschluss erscheint folgende Meldung:



Schützen Sie Ihre Unternehmens-Rechner

Die folgenden Schritte zeigen Ihnen, wie Sie das Risiko von Datenverlust und anderen durch Ransomware-Angriffe verursachte Schäden minimieren können.

11 SCHRITTE ZUM SCHUTZ VOR DATENVERLUST

1. Erstellen Sie regelmäßig Backups von wichtigen Daten
2. Aktivieren Sie die automatische Aktualisierung Ihrer Software
3. Schulen Sie Ihre Mitarbeiter
4. Lassen Sie sich bekannte Dateierweiterungen anzeigen
5. Blockieren Sie E-Mails anhand der Dateiendungen im Anhang
6. Deaktivieren Sie die Dateiausführung aus AppData/LocalAppData-Ordnern
7. Genießen Sie freigegebene Ordner mit besonderer Vorsicht
8. Deaktivieren Sie RDP
9. Nutzen Sie ausschließlich branchenführende Sicherheitslösungen
10. Nutzen Sie die Systemwiederherstellung, um das System auf einen sauberen Stand zurückzusetzen
11. Nutzen Sie ein Standardkonto ohne Administratorrechte

1. Erstellen Sie regelmäßig Backups von wichtigen Daten

Regelmäßige Backups sind eine simple aber effektive Methode zum Schutz Ihrer Daten vor Ransomware und anderem Schadcode. Zumal neuere Malware auch Dateien auf Netzlaufwerken mit zugeordneten Laufwerksbuchstaben und teilweise auch auf verfügbaren Ablagen im Netzwerk verschlüsseln kann.

Darunter zählen alle externen Laufwerke wie USB-Sticks sowie andere Netzwerk- oder Cloud-Datenspeicher. Für regelmäßige Backups empfehlen wir, ein gesondertes Gerät zu nutzen, um die Daten getrennt von den Produktivnetzen zu speichern. Testen Sie die Wiederherstellung von Daten in regelmäßigen Abständen. So stellen Sie sicher, dass Daten verfügbar sind und Sie im Ernstfall routinemäßig reagieren können.

2. Aktivieren Sie die automatische Aktualisierung Ihrer Software

Malware-Autoren wissen, dass veraltete Software eine der häufigsten Schwachstellen bei Anwendern ist. Sie nutzen darin bekannte Sicherheitslücken aus und greifen so unbemerkt auf Firmengeräte und -systeme zu. Regelmäßige Patches und Updates der verwendeten Software und Geräte erhöhen den Schutz gegen Ransomware um ein Vielfaches.

In der Regel werden Sicherheits-Updates von Software-Anbietern in regelmäßigen Abständen bereitgestellt. Bei kritischen Schwachstellen kommt es allerdings auch zu außerplanmäßigen Aktualisierungen. Aktivieren Sie daher – wenn möglich – automatische Updates oder besuchen Sie die Webseite des Anbieters. Konfigurieren Sie zusätzlich eine Alarmfunktion im Falle neuer kritischer Schwachstellen und wichtiger Patches.

3. Schulen Sie Ihre Mitarbeiter

Eines der schwächsten Glieder in der Sicherheitskette ist der Mensch selbst. Betrüger wenden oft sogenannte Social Engineering-Methoden an, um Mitarbeiter zur Preisgabe von vertraulichen Informationen und zur Ausführung schädlicher Programme zu bewegen. Gefälschte E-Mails von Lieferunternehmen oder Banken und als interne E-Mails getarnte Nachrichten sind Klassiker, um Mitarbeiter zu täuschen. Die Erhöhung des Sicherheitsbewusstseins durch Schulungen und Trainings helfen der Belegschaft, verdächtige E-Mails zu erkennen und mit darin enthaltenen Anhängen oder Links vorsichtig umzugehen.

4. Lassen Sie sich bekannte Dateierweiterungen anzeigen

Ransomware wird in vielen Fällen als E-Mail-Anhang mit der Endung „.PDF.EXE" verbreitet. Kritisch dabei ist, dass Windows standardmäßig bekannte Dateierweiterungen ausblendet. Aktivieren Sie die Anzeige der gesamten Dateiendungen im Explorer, um verdächtige Dateien besser erkennen zu können.

5. Blockieren Sie E-Mails anhand der Dateiendungen im Anhang

Ist Ihr Gateway-Mail-Scanner in der Lage, Dateien anhand ihrer Endung zu filtern, können Sie E-Mails mit offensichtlichen oder versteckten angehängten ausführbaren Dateien („.EXE"- bzw. „*.*.EXE"-Dateien) blockieren. Wir raten Ihnen, Dateien mit folgenden Endungen ebenfalls zu filtern: *.BAT, *.CMD, *.SCR und *.JS.

6. Deaktivieren Sie die Dateiausführung aus AppData/LocalAppData-Ordnern

In einigen Fällen starten Ransomware-Varianten ihre ausführbaren Dateien vom AppData- oder LocalAppData-Order aus. Innerhalb von Windows oder mithilfe einer Intrusion Prevention Software können Sie Regeln festlegen, um solche Ausführungen zu verhindern. Startet eine legitime Software aus bestimmten Gründen nicht vom regulären Programmordner, sondern vom AppData-Ordner aus, können hierfür Ausnahmen definiert werden.

7. Genießen Sie freigegebene Ordner mit besonderer Vorsicht

Wird ein Unternehmensgerät mit Ransomware infiziert, können auch Dateien in freigegebenen Ordnern verschlüsselt werden, sofern der betroffene Nutzer Schreibrechte besitzt. Aus diesem Grund ist es entscheidend, dass Ihre Mitarbeiter darauf achten, welche Dateien sie auf freigegebenen Laufwerken speichern, da diese durch infizierte Systeme ebenfalls verschlüsselt werden können.

8. Deaktivieren Sie RDP

In vielen Fällen nutzt Ransomware das Remote Desktop Protocol (RDP), um Zugang zum anvisierten Gerät zu erlangen. Hierbei handelt es sich um ein Windows-Dienstprogramm, das einen Fernzugriff auf den Rechner ermöglicht. Darüber hinaus verwenden Cyberkriminelle das Tool zur Ausschaltung von Sicherheitssoftware. Deaktivieren Sie RDP, sofern Sie es nicht benötigen. Eine Anleitung dazu finden Sie in den entsprechenden Knowledge-Base-Artikeln von Microsoft.

9. Nutzen Sie ausschließlich branchenführende Sicherheitslösungen

Malware-Autoren verbreiten regelmäßig neue Varianten ihrer schädlichen Codes, um eine Erkennung durch Sicherheitssoftware zu vermeiden. Hat sich eine Malware auf einem System eingenistet, wartet sie in vielen Fällen auf weitere Anweisungen von ihrem Command and Control (C&C) Server, bevor sie ihre schädlichen Funktionen ausführt. Das hat den Vorteil, dass selbst wenn Ransomware nicht vom Antivi-

ren-Modul erkannt wird, sie vor Beginn des Verschlüsselungsprozesses der Daten über die Kommunikation mit dem C&C-Server identifiziert werden kann. Die neueste ESET Sicherheitssoftware verfügt über einen erweiterten **Schutz vor Botnets,** der die schädliche Kommunikation erkennt und den entsprechenden Prozess blockiert.

10. Nutzen Sie die Systemwiederherstellung, um das System auf einen sauberen Stand zurückzusetzen

Ist die Systemwiederherstellung auf dem infizierten Windows-Gerät aktiviert, lässt sich das System auf den letzten bekannten, sauberen Stand zurücksetzen. Einige der verschlüsselten Dateien können eventuell aus der Sicherung wiederhergestellt werden. Hier müssen Sie unverzüglich handeln.

Eine Reihe neuerer Ransomware-Varianten löschen die Wiederherstellungspunkte aus der Systemwiederherstellung, sobald der Schadcode gestartet wird. Meist geht dieser Vorgang unbemerkt von statten, weil sich diese Prozeduren unter Windows auch ohne Wissen des Nutzers ausführen lassen.

11. Nutzen Sie ein Standardkonto ohne Administratorrechte

Die Nutzung eines Kontos mit Administratorrechten birgt immer ein Sicherheitsrisiko, weil sich auch Malware diese Rechte zunutze machen und das System noch leichter infizieren kann. Nutzen Sie daher für alltägliche Aufgaben Nutzerkonten mit eingeschränkten Rechten und das Administratorkonto nur in Ausnahmefällen. Deaktivieren Sie keinesfalls die Benutzerkontensteuerung.

RANSOMWARE: WIE SIE FUNKTIONIERT

Ransomware ist eine schädliche Software, die Ihr Gerät sperren und wertvolle, vertrauliche Dateien verschlüsseln kann.

Die Schadsoftware wird häufig über E-Mail oder als Drive-by-Download auf manipulierten Webseiten verbreitet. Nach erfolgreicher Ausführung sperrt die Ransomware den Zugang zum System und zeigt eine Popup-Nachricht mit einer Lösegeldforderung an.

Was tun, wenn mein Rechner bereits infiziert ist?

Isolieren Sie das Gerät

Führen Sie oder einer Ihrer Mitarbeiter eine verdächtige Datei aus und lassen sich daraufhin einige Ihrer gespeicherten Dateien nicht mehr öffnen, trennen Sie das Gerät umgehend vom Internet, vom Firmennetzwerk und falls möglich von der Stromversorgung. Dadurch kann die Kommunikation zwischen Malware und C&C-Server noch vor Beginn des Verschlüsselungsprozesses von Dateien und Laufwerken unterbunden werden.

Auch wenn es sich dabei um keine sichere Methode handelt, besteht zumindest die Chance, dass einzelne wertvolle Dateien vor der kompletten Verschlüsselung bewahrt werden. Wir raten Ihnen, das System über die Hardware abzuschalten. Womöglich wurde die Ransomware so programmiert, dass sie beim normalen Herunterfahren der Software noch mehr Schaden anrichtet.

Kontaktieren Sie den technischen Support von ESET

Kontaktieren Sie ihren technischen Ansprechpartner bzw. den Support von ESET, wenn Sie von einer Ransomware-Variante betroffen sind und über kein aktuelles Backup verfügen. Reichen Sie auch ein Protokoll vom ESET Log Collector und einige Samples der verschlüsselten Dateien ein – am besten etwa fünf MS Word- oder Excel-Dateien.

Sind Sie Inhaber von mindestens 100 Lizenzen, können Sie Kontakt mit unseren Experten aufnehmen. Nach Erstellung eines Helpdesk-Tickets über unser Onlinesystem werden sie anschließend zum Vorfall befragt. In Zusammenarbeit mit dem ESET Research Lab setzen unsere Experten alles daran, Ihre übermittelten Dateien zu entschlüsseln und wiederherzustellen.

Keine leichte Aufgabe, denn die Entwickler solcher Schadcodes nutzen immer stärkere Verschlüsselungstechniken, um Ransomware noch effektiver zu machen. In vielen Fällen besteht kaum eine Chance, alle Dateien wieder zu entschlüsseln.

Verschlüsselung ist heutzuage technologischer Standard beim Schutz von finanziellen Transaktionen – ob bei Banken, E-Shops oder anderen Online-Diensten und nahezu unüberwindbar. Aus diesem Grund kann kein Anbieter die Wiederherstellung Ihrer Dateien garantieren.

Die ESET-Experten werden nach Schlupflöchern in der Ransomware suchen, die es Ihnen mit etwas Glück ermöglicht, den Schaden an Ihren Laufwerken und Geräten zu beheben. Sind sie erfolgreich, erhalten Sie ein für Ihr Unternehmen maßgeschneidertes Entschlüsselungs-Tool.

ESET-Analysen zufolge ist das in einem von fünf Ransomware-Fällen möglich. Je nach Komplexität der Malware kann dieser Prozess mehrere Wochen andauern. Die Erfolgsquote ist in vielen Fällen gering. Kunden unseres neuen ESET Premium Supports stehen unsere Experten an 365 Tagen rund um die Uhr mit Rat und Tat zur Seite.

Behalten Sie auch die Android-Geräte im Blick

Wie eingangs erwähnt, haben es Malware-Autoren nicht ausschließlich auf Windows-Systeme abgesehen. In den letzten Jahren ist das marktführende mobile Betriebssystem *Android* mehr und mehr in den Fokus gerückt, das auf vielen Unternehmens-Smartphones und -Tablets läuft.

ESET entdeckte bereits eine Vielzahl an Ransomware-Familien für Android, die gezielt mobile Geräte infizieren. Angreifer nutzen verschiedene Techniken, geben sich beispielsweise als Antiviren-Software aus oder tarnen die Lösegeldforderung als Meldung einer Polizeibehörde und blockieren dann das Gerät, wie im Fall von *Reveton*.

2014 identifizierten unsere Experten erstmals eine Ransomware, die in der Lage war, *Dateien auf Android-Mobilgeräten zu verschlüsseln*. Mittlerweile wurden mehr als 50 weitere, viel komplexere und raffiniertere Varianten entwickelt. Nur ein Jahr später tauchte der *erste Schädling* auf, der durch die Erstellung eines beliebigen vierstelligen Entsperrungscodes den Zugriff auf das Gerät blockierte.

Alle Varianten dieser Schadcodes konnten den Zugang zu wichtigen Geschäftsressourcen verhindern und verlangten von den Opfern der Unternehmen riesige Summen für die Wiederherstellung der Daten.

WIE SIE IHRE MOBILE ANDROID-FLOTTE SCHÜTZEN

A. Schulen Sie Ihre Mitarbeiter

Erhöhen Sie das Sicherheitsbewusstsein Ihrer Mitarbeiter hinsichtlich der Android-Gefahren, damit auch sie Schutzmaßnahmen ergreifen. Schulungen sind ein wichtiger Schritt zur Absicherung.

- Laden Sie keine Dateien oder Anwendungen aus inoffiziellen App-Stores und von dubiosen Drittanbieten herunter.
- Beim Download aus offiziellen Stores lesen Sie die Bewertungen anderer Nutzer. Tritt schädliches Verhalten bei einer App auf, lässt sich dies in der Regel in den Kommentaren nachlesen.
- Mitarbeiter sollten überprüfen, welche Berechtigungen eine Anwendung fordert und hinterfragen, ob sie für die Funktionsfähigkeit tatsächlich notwendig sind.
- Falls möglich, erstellen Sie eine Liste mit allen Apps, die Mitarbeiter auf ihren Firmengeräten installieren dürfen oder administrieren Sie Ihre Geräte über eine zentrale Mobile Device Management (MDM) Lösung.

B. Nutzen Sie eine Sicherheitssoftware

Installieren Sie eine mobile Sicherheits-App und halten Sie sie auf allen Firmengeräten stets aktuell. Als ESET-Kunde können Sie die ESET Endpoint Security für Android als Bestandteil folgender Business-Lösungen einsetzen:

- ESET Endpoint Protection Standard
- ESET Endpoint Protection Advanced
- ESET Secure Business
- ESET Secure Enterprise

C. Nehmen Sie regelmäßige Backups vor

Hinzu kommt die Erstellung regelmäßiger Backups aller wichtigen Daten auf Android-Geräten. Auch wenn durch die oben genannten Sicherheitsvorkehrungen die Risiken eines Ransomware-Angriff minimiert werden, bieten Backups zusätzlichen Schutz und verhindern im Fall des Falles größeren Schaden.

Was tun, wenn mein Android-Gerät bereits infiziert ist?

Wurde Ihr Gerät oder das Ihres Mitarbeiters durch Ransomware infiziert, gibt es je nach Malware-Familie verschiedene Optionen zur Beseitigung.

1. Im abgesicherten Modus starten

Bei weniger komplexen bildschirmsperrenden Ransomware-Varianten ist häufig ein Neustart des Geräts im abgesicherten Modus ausreichend. Drittanbieter-Apps (einschließlich der Malware) werden auf diese Weise nicht geladen und die schädliche Anwendung lässt sich einfach deinstallieren. Die Schritte für einen Neustart im abgesicherten Modus können je nach Gerätemodell variieren. Informationen dazu finden Sie im Geräte-Handbuch oder in diversen Tutorials und Artikeln im Internet.

2. Widerrufen Sie die Administratorenrechte für Malware

Neuere Ransomware-Familien sind in der Lage, die Administratorrechte für das Gerät zu erlangen. Bevor die App deinstalliert werden kann, müssen Sie diese innerhalb der Einstellungen widerrufen.

3. Setzen Sie das Passwort über den Gerätemanager zurück

Hat eine mit Administratorenrechten ausgestattete Ransomware den Zugriff auf Ihr Gerät gesperrt, ist die Situation etwas komplizierter. Unter Umständen kann die Sperre aber mithilfe von Googles Android-Gerätemanager oder einer alternativen Mobile Device Management-Lösung aufgehoben werden.

4. Kontaktieren Sie den technischen Support

Wurden die Dateien auf Ihrem Gerät durch eine Crypto-Ransomware wie Android/Simplocker verschlüsselt, kontaktieren Sie umgehend den technischen Support Ihres Sicherheits-Anbieters. Je nach Variante lassen sich die Dateien unter Umständen wieder entschlüsseln.

5. Setzen Sie das Gerät auf die Werkseinstellungen zurück

Blieben alle bisherigen Versuche erfolglos, hilft im Notfall nur noch das Zurücksetzen auf die Werkseinstellungen. Dabei werden alle Daten auf dem Gerät gelöscht.

Zu guter Letzt: Soll ich das Lösegeld bezahlen?

ESET rät Unternehmen und Privatanwendern gleichermaßen, **auf die Lösegeldforderungen nicht einzugehen**.

Bei den Erpressern handelt es sich um Kriminelle. Es gibt keine hundertprozentige Sicherheit, dass nach Zahlung des Lösegelds die betroffenen Daten oder Geräte tatsächlich wieder entschlüsselt bzw. entsperrt werden.

Hinzu kommt, dass Sie damit die Erpresser – und gegebenfalls weitere kriminelle Aktivitäten – finanziell unterstützen.

Selbst wenn die Angreifer Ihnen einen Entschlüsselungscode zukommen lassen haben, gibt es keine Garantie dafür, dass er funktioniert. ESET-Analysen haben dies mehrmals belegt. Etliche Male wurde der von der Ransomware generierte PIN-Code zur Entsperrung des Android-Geräts gar nicht erst an die Erpresser übermittelt. So hatten die Opfer niemals eine Chance, den Zugang zu Ihrem Gerät wiederzuerlangen.

Hinzu kommt, dass durch Ihre Zahlungsbereitschaft ein weiterer Angriff nicht ausgeschlossen ist, um noch mehr Geld zu erbeuten.