F-SECURE CLOUD PROTECTION FÜR MICROSOFT OFFICE 365

Lösungsübersicht

F-Secure

INHALT

Mai 2020

ZUSAMMENFASSUNG

F-Secure Cloud Protection für Microsoft Office 365 hilft Firmen bei der Risikominimierung bei geschäftlichen E-Mails durch einen wirksamen Schutz für Microsoft Office 365 vor immer raffinierteren Phishing-Angriffen und böswilligen Inhalten. Die nahtlose Cloud-to-Cloud-Integration macht Middleware oder teuren IT-Support überflüssig und F-Secure Cloud Protection so zu einer kostengünstigen, benutzerfreundlichen Lösung.

F-Secure Cloud Protection für Microsoft Office 365 wird von Unternehmen mit folgenden Anforderungen bevorzugt:

- Minimierung von Geschäftsunterbrechungen durch Reduzierung der E-Mail-Risiken aufgrund schädlicher Inhalte, die vom Standard-E-Mail-Schutz von Microsoft Office 365 nicht erkannt werden.
- Kostengünstige Lösung zum Schutz von Microsoft Exchange Online Postfächern vor Phishing-Angriffen, internen E-Mail-Risiken sowie bösartigen Inhalten und Links.
- Cloud-to-Cloud-Integration mit einfacher Bereitstellung und nahtloser Verwaltung zur Gewährleistung eines unterbrechungsfreien und effizienten Schutzes vor E-Mail-Bedrohungen.

F-Secure Cloud Protection für Microsoft Office 365 bietet Sicherheitsfunktionen zur Minderung von Risiken, die von gemeinsam genutzten Dateien und URLs in Exchange Online Postfächern genutzt werden. Wenn ein Endbenutzer Microsoft-Outlook-Elemente wie E-Mails, Termine, Aufgaben, Kontakte oder Notizen in seinem Postfach empfängt oder erstellt, analysiert der F-Secure Cloud Protection Service alle enthaltenen Anhänge und Links auf schädliche Inhalte wie Malware, Trojaner, Ransomware oder Phishing. Außerdem offeriert die Lösung umfangreiche Berichtsfunktionen, fortschrittliche Sicherheitsanalysen und Systemereignisse, um eine schnellere Reaktion auf die identifizierten Bedrohungen zu gewährleisten. F-Secure Cloud Protection für Microsoft Office 365 umfasst ein Managementportal für die tägliche Verwaltung und ein Service-Back-End, das die Security Cloud von F-Secure zur Analyse der Microsoft-Office-365-Elemente auf bösartige Dateien und URLs nutzt. Sie müssen keine zusätzliche Software installieren oder Änderungen an Ihrer Netzwerkkonfiguration vornehmen, um die Lösung verwenden zu können.

F-Secure hat die Auszeichnung „Best Protection“ von AV-Test im Laufe des achtjährigen Bestehens des Instituts, nicht weniger als sechs* Mal erhalten. AV-Test führt das ganze Jahr über Vergleichsprüfungen durch. Um diese wertvolle Auszeichnung zu bekommen, sind konstant gute Ergebnisse bei den Schutztests erforderlich.

Um diese anspruchsvollen Standards zu erfüllen, verwendet die Software einen mehrschichtigen Sicherheitsansatz und nutzt verschiedene moderne Technologien, darunter heuristische und verhaltensbasierte Gefahrenanalysen sowie Echtzeit-Bedrohungsinformationen, die die Security Cloud von F-Secure bereitstellt. Das garantiert, dass sich der Kunde stets auf eine optimale Sicherheitsleistung verlassen kann.

1. MODELL DER GEMEINSAMEN VERANTWORTLICHKEIT

Einige Unternehmen gehen davon aus, dass beim Kauf eines Cloud-Dienstes der Anbieter auch für die Sicherheit verantwortlich ist. Das stimmt aber nur zum Teil. Bei Cloud-Services gibt es ein Prinzip, das als Modell der gemeinsamen Verantwortlichkeit bezeichnet wird. Es besagt, dass Cloud-Anbieter für die Sicherheit der Cloud AN SICH verantwortlich sind – und Kunden, die die Cloud nutzen, für die Sicherheit IN der Cloud. In der Praxis bedeutet dies, dass der Cloud-Anbieter für die physische Sicherheit der Rechenzentren sorgt, damit niemand physisch in ihre Einrichtungen einbrechen und die Sicherheit der zugrunde liegenden Plattform untergraben kann. Cloud-Anbieter kümmern sich auch um die Authentifizierung, Identifizierung sowie Benutzer- und Admin-Kontrollen. Im Sinne der DSGVO gelten Cloud-Anbieter als Datenverarbeiter.

Kunden, die Cloud-Services nutzen, sind für die Sicherheit der dort gespeicherten Daten verantwortlich. Deshalb müssen sie dafür sorgen, dass keine bösartigen Inhalte, gezielten Angriffe, internen Sicherheitsrisiken, Täuschungen oder Social Engineering vorliegen, indem sie ihre Mitarbeiter in Sicherheitsschulungen schicken. Kunden, die Cloud-Dienste in Anspruch nehmen, sind für die Sicherheit ihrer Mails selbst verantwortlich. Denn sie sind nach DSGVO Datenbesitzer.

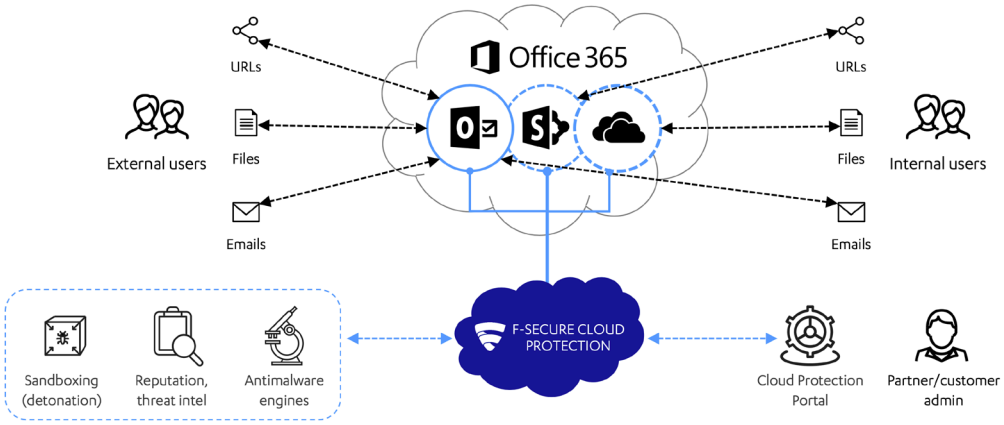
F-Secure Cloud Protection für Microsoft Office 365 bietet:

- Eine **kostengünstige** Anwendung zum Schutz von Microsoft-Office-365-E-Mails vor Phishing-Angriffen, internen Risiken sowie bösartigen Inhalten und URLs.
- In Kombination mit dem preisgekrönten Endgeräteschutz sowie den Erkennungs- und Reaktionsfunktionen von F-Secure bietet die Lösung einen **umfassenderen Schutz** für Ihr Unternehmen als jedes E-Mail-Sicherheitsprogramm allein.
- **Cloud-to-Cloud-Integration** mit einfacher Bereitstellung und nahtloser Verwaltung zur Gewährleistung eines unterbrechungsfreien und effizienten Schutzes vor E-Mail-Bedrohungen.

2. LÖSUNGSÜBERSICHT

F-Secure Cloud Protection für Microsoft Office 365 fungiert als cloudbasierter Sicherheitsservice, der die Risiken für geschäftliche E-Mails reduziert, indem er einen wirksamen Schutz vor internen Bedrohungen, Phishing-Angriffen sowie bösartigen Inhalten und URLs im ein- und ausgehenden Datenverkehr für Microsoft-Office-365-E-Mail-Nachrichten aufbaut. Zusätzlich zu E-Mail-Nachrichten werden auch andere Exchange-Elemente wie Aufgaben, Kalendertermine, Kontakte und Kurznotizen auf bösartige Inhalte und URLs überprüft.

Das folgende Diagramm verschafft Ihnen einen groben Überblick darüber, wie die Lösung Microsoft Office 365 in der Praxis besser schützt.



Dateien, URLs oder E-Mails

F-Secure Cloud Protection für Microsoft Office 365 benutzt die Postfächer von MS-O-365-Usern, um Dateianhänge und Weblinks zu analysieren. Diese können im Text und im Header von Exchange-Elementen wie E-Mails, Kalenderterminen, Aufgaben, Kontakten und Kurznotizen im eingehenden, ausgehenden und internen Datenverkehr enthalten sein.

F-Secure Security Cloud (Sandboxing, Reputation Threat Intelligence, Anti-Malware-Engines)

F-Secure Security Cloud verwendet eine mehrstufige Inhaltsanalyse in einem abgestuften Prozess, der auf dem Risikoprofil des jeweiligen Inhalts basiert. Zusätzlich werden riskante Dateien mit unserer Cloud-Sandboxing-Technologie einer tieferen Analyse unterzogen, wodurch Zero-Day-Malware-Angriffe und andere hoch entwickelte Gefahren im Keim erstickt werden.

F-Secure Cloud Protection für Microsoft-Office-365-Managementportal

Das Protection-Portal dient Admins zur Verwaltung des Dienstes beim Schutz von MS-O-365-Inhalten. Das Management-Portal besteht aus Analyse- und Systemereignisfunktionen, die dabei helfen, die Bedrohungen auf Grundlage der im Portal bereitgestellten Informationen zu priorisieren und Sicherheitsrisiken zu mindern. Das Portal verfügt auch über Dashboard- und Berichterstattungsfunktionen, die den Status des Systems jederzeit überprüfen und protokollieren. Die Berichte stehen zum Download und zum einfachen Austausch zur Verfügung.

Partner- und Kunden-Administratoren

Der F-Secure Cloud Protection für Microsoft Office 365-Dienst erlaubt es Partnern und Kunden die Sicherheitswarnungen und E-Mail-Benachrichtigungen zu verwalten und für die bei der Analyse der Postfächer gefundenen bösartigen Inhalte, je nach Schwere der Warnung oder der Bedrohungskategorie, geeigneten Maßnahmen zu ergreifen.

Managementrollen

Dem Administrator von F-Secure Cloud Protection für Microsoft Office 365 kann – je nach Verwaltungsanforderung – im Portal eine bestimmte Rolle zugewiesen werden. Der Dienst erlaubt die Rollen „Admin", „Quarantine Manager" und „Read-only". Jede Rolle definiert Berechtigungen, die dem jeweiligen Benutzer Zugriff auf spezielle Verwaltungsfunktionen des Portals ermöglichen. Der User mit der„Admin"-Rolle kann über das webbasierte Benutzerverwaltungsportal von F-Secure Business diverse Benutzerrollen beifügen oder entfernen. Dasselbe Benutzerkonto kann für den Zugriff auf andere F-Secure-Produkte und Managementportale verwendet werden, indem der Zugang auf die jeweilige Lösung über das F-Secure-Business-Portal hinzugefügt wird.

Benutzer

Interne und/oder externe Benutzer werden während sie Elemente wie E-Mails, Kalendereinträge, Aufgaben, Kontakte, Haftnotizen usw. in ihren Postfächern erstellen bzw. austauschen, aktiv durch den Dienst F-Secure Cloud Protection for Microsoft Office 365 geschützt. Jede geschützte Mailbox wird bei eingehenden, ausgehenden und internen Datenverkehr auf schädliche Inhalte in Exchange-Elementen gescannt.

2.1. Dateischutz

F-Secure Cloud Protection für Microsoft Office 365 scannt Inhalte in Dateianhängen in Exchange-Elementen, um vor Viren, Trojanern, Ransomware und anderer hoch entwickelter Malware zu schützen. Der Schutz arbeitet im Vergleich zu herkömmlichen Technologien weitaus besser, da er Echtzeit-Bedrohungsinformationen nutzt, die von Zigmillionen Sicherheits-Clients gesammelt wurden. Dadurch bietet er eine schnellere und effektivere Abschirmung vor neuen Gefahren.

2.1.1. Erstanalyse

Das Back-End von F-Secure Cloud Protection erhält die Prüfsumme (SHA1) der Dateianhänge, die sich in den MS-O-365-Exchange-Elementen (E-Mail, Kalender, Termine, Kurznotizen usw.) befinden. Die Prüfsumme wird mit denen verglichen, die im vorhandenen Cache zur Erkennung von Bedrohungen im Back-End gespeichert sind, um festzustellen, ob die Datei bereits zuvor analysiert wurde. Wenn Analyseergebnisse aus dem Cache vorliegen, werden sie automatisch verwendet und es sind keine weiteren Untersuchungen notwendig. Vorhandene Erkenntnisse der Bedrohungserkennung erfahren eine regelmäßige Aktualisierung, nicht mehr aktuelle Werte werden automatisch gelöscht. Das gewährleistet stets einen aktuellen Schutz.

2.1.2. Prüfung der Bedrohungsinformationen

Falls im Cache keine Ergebnisse vorliegen, werden über die Security Cloud von F-Secure unter Verwendung der SHA-256-Prüfsumme die Bedrohungsinformationen überprüft. Der Dienst gibt die Sicherheitsreputation der Datei, die Verbreitung und mögliche erkannte Bedrohungen zurück. Abhängig von den Richtlinieneinstellungen entfernt das System entweder den Dateianhang oder das gesamte Exchange-Element, optional können Anhang oder Element auch unter Quarantäne gestellt werden, sowie eine Benachrichtigung an den Benutzer und/oder Administrator versandt werden.

2.1.3. Multi-Engine-Anti-Malware

Falls sich die Datei als unbekannt erweist, wird ihr Inhalt zur weiteren Bedrohungsuntersuchung auf die Security Cloud von F-Secure hochgeladen. Mehrere sich ergänzende Anti-Malware-Engines unterziehen sie einer eingehenderen Analyse, um Malware, Zero-Day-Exploits und komplexe Gefahrenmuster zu finden. In diesem Stadium nutzt der Analyseprozess den kompletten Umfang der von den F-Secure Labs gesammelten Bedrohungsdaten und -funktionen.

2.1.4. Erweiterte Bedrohungsanalyse (Sandbox)

Auf Basis der Ergebnisse der Bedrohungsanalyse verwendet das System fein abgestimmte Verfahren des maschinellen Lernens, um zu entscheiden, ob die Datei zur genaueren Durchsicht in die Cloud-Sandbox gesendet werden soll. Falls eine Datei verdächtige Risikoindikatoren aufweist, gelangt sie in die Sandbox, wo sie für eine Verhaltensanalyse in mehreren virtuellen Umgebungen ausgeführt wird. Durch die Fokussierung auf bösartiges Verhalten statt auf statische Parameter kann die Cloud-Sandbox selbst die komplexesten Zero-Day-Attacken identifizieren und blockieren.

2.1.5. Analyseergebnisse

Abschließend wird der Dateianhang entweder als schädlich oder sauber eingestuft. Je nach Voreinstellung wird die Datei aus dem Exchange-Element entfernt, wenn sie schädlich oder verdächtig ist, und/oder der Benutzer und die Administratoren bekommen eine Nachricht zu dem Vorfall. Falls nichts Verdächtiges auffällt, ist die
Datei in ihrem ursprünglichen Exchange-Element zugänglich. Die Einstufung der Datei und andere Details der Bedrohungsanalyse werden im Bedrohungserkennungs-Cache zur zukünftigen Verwendung im Service-Back-End gespeichert.

2.2. URL-Schutz

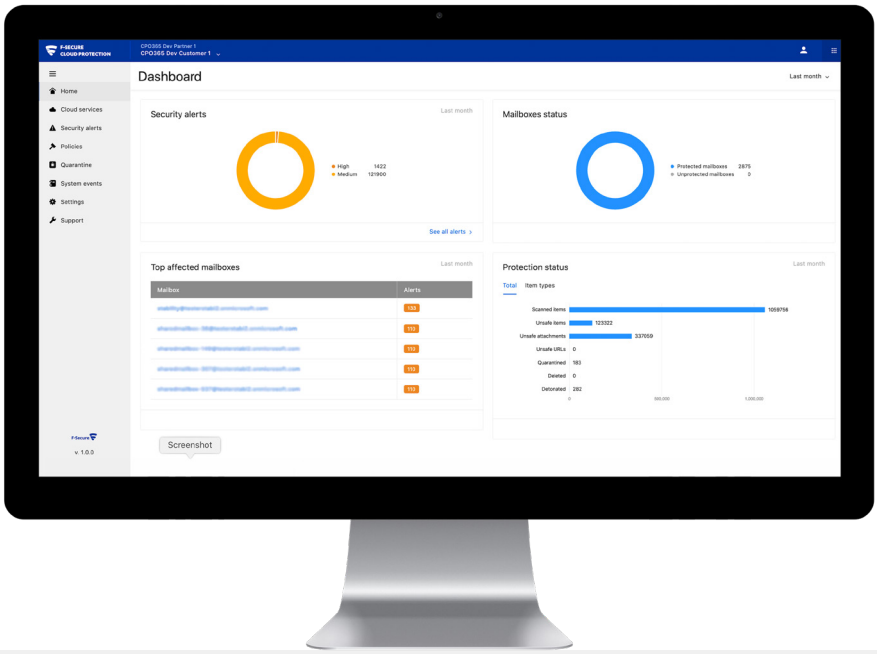
Der URL-Schutz gehört zu den wichtigsten Sicherheitsfunktion. Er verhindert proaktiv, dass Benutzer von MS O 365 über Weblinks, die zu Exchange-Elementen wie E-Mails, Kalenderterminen, Aufgaben, Kontakten oder Kurznotizen hinzugefügt werden, auf bösartige oder unerwünschte Inhalte zugreifen. Dies macht ihn zu einem besonders effektiven Sicherheitsfeature, da ein frühzeitiges Eingreifen die allgemeine Gefährdung durch aggressive Inhalte und damit Angriffe erheblich reduziert. So unterbindet er beispielsweise, dass Benutzer dazu verleitet werden, auf scheinbar legitime Phishing-Websites und hinterlistige Websites zuzugreifen.

Der URL-Schutz wurde entwickelt, um effizient mit den Milliarden im Internet verfügbaren Websites und ihrem ständig schwankenden Sicherheitsstatus umzugehen. Er basiert auf Echtzeit-Suchabfragen an die Security Cloud von F-Secure. Alle Ermittlungen durchlaufen mehrere Anonymisierungsebenen, um die größtmögliche Geschäftsvertraulichkeit zu gewährleisten.

Die Abfrage ruft die aktuelle Reputation der Websites und ihrer Dateien auf Grundlage verschiedener Datenparameter ab. Dazu zählen IP-Adressen, URL-Schlüsselwörter, Website-Muster, extrahierte Website-Metadaten wie iframes und Dateitypen sowie Website-Verhalten, Exploit-Versuche, bösartige Umleitungen oder Skripte.

2.2.1. URL-Sicherheitsüberprüfung

Die Lösung scannt den Hauptteil der Exchange-Elemente und fragt die Reputation der enthaltenen URLs von der Security Cloud von F-Secure ab. Ergibt die Anfrage eine Einstufung als bösartig, wird der Zugriff auf die URL entweder blockiert oder erlaubt – je nach Richtlinieneinstellung. Der Administrator kann die Richtlinie so konfigurieren, dass der Zugriff auf die URL zugelassen wird, indem er den Benutzer im Betreff des Exchange-Elements über die Einschätzung der URL informiert. Der Administrator kann die Richtlinie aber auch so einstellen, dass der Zugriff blockiert wird, indem er das Element unter Quarantäne stellt. Alternativ kann er es auch löschen, falls sich die URL als heimtückisch oder verdächtig erweist.



2.3. Managementportal

F-Secure Cloud Protection für Microsoft Office 365 unterstützt Administratoren bei der Verwaltung von MS-O-365-Exchange-Umgebungen.

Umfangreiche Berichte, flexible Warnmeldungen und moderne Sicherheitsanalysen machen es Administratoren einfach, auf Bedrohungen zu reagieren. Die vollständige 360-Grad-Rundumsicht stellt sicher, dass sie ihre MS-O-365-Nutzungsmuster kennen. Dies hilft bei der Abwehr eines Angriffs, bei der Untersuchung einer Attacke von einer unbekannten Quelle oder der Überprüfung, ob MS O 365 Teil eines Zwischenfalls war.

2.3.1. Einrichtung

F-Secure Cloud Protection für Microsoft Office 365 unterstützt die Cloud-to-Cloud-Integration, ohne dabei zusätzliche Software installieren oder Änderungen auf dem Server oder den Clients vornehmen zumüssen. Die Schutzfunktion ist plattformunabhängig und in der Lage, Bedrohungen zu erkennen – unabhängig davon, welches Gerät oder welche Anwendung für den Zugriff auf die Exchange-Postfachelemente zum Einsatz kommt. Adminis können den Service für das Scannen der MS-O-365-Exchange-Benutzerpostfächer konfigurieren und in nur wenigen Minuten umfassenden Schutz einrichten.

2.3.2. Dashboard

F-Secure Cloud Protection für Microsoft Office 365 verfügt über ein benutzerfreundliches Dashboard für den schnellen Zugriff auf die neuesten Sicherheitswarnungen zu verdächtigen Inhalten, die in den verwalteten Umgebungen gefunden wurden. Aber auch die am stärksten betroffenen Postfächer mit der höchsten Anzahl an Sicherheitsvorfällen sowie stets aktuelle Daten gescannter Exchange-Elemente und die Art der Maßnahmen gegen diese stehen im Fokus.

Das Dashboard zeigt auch die Absicherung der Umgebung in Bezug auf die Anzahl der durch den Sicherheitsdienst geschützten beziehungsweise nicht geschützten Postfächer an. So wissen Sie jederzeit, ob im Umfeld Sicherheitsdefizite aufgrund ungeschützter Postfächer existieren.

2.3.3. Sicherheitswarnungen

Das Sicherheitswarnungs-Widget verschafft einen schnellen und simplen Zugriff auf die neuesten Sicherheitsmeldungen, sortiert nach ihrem Schweregrad. Die sortierte Liste hilft dem Administrator bei der sofortigen Priorisierung von Hochrisikoalarmen mit detaillierten Informationen zu den aufgespürten Inhalten in den Postfächern der User.

2.3.4. Postfachstatus

Das Postfachstatus-Widget auf dem Dashboard meldet die Anzahl der geschützten und ungeschützten Postfächer der Firma in MS O 365. Auf diese Weise kann der Administrator jederzeit nachvollziehen, ob Sicherheitslücken vorhanden sind.

2.3.5. Am häufigsten angegriffene Postfächer

Das Widget für die am häufigsten angegriffenen Postfächer im Dashboard listet die fünf Accounts mit den meisten Warnzeichen auf. Es hilft bei der Prüfung, ob die Zahl der Sicherheitswarnungen für bestimmte Postfächer plötzlich ansteigt, was auf einen möglichen Sicherheitsvorfall hindeuten könnte.

2.3.6. Schutzstatus

Das Schutzstatus-Widget zeigt die Gesamtanzahl der gescannten und unsicheren Elemente an. Das Widget veranschaulicht auch die Art der Maßnahmen, die zum Schutz vor der feindlichen Attacke ergriffen wurden, etwa das Löschen. Die Elementtypen-Registerkarte im Widget bietet nähere Informationen über den bösartigen Inhalt, der pro Elementtyp (E-Mails, Kalendertermine, Aufgaben, Kurznotizen, Kontakte, Gruppen und andere) im Postfach gefunden wurde.

2.3.7. Schutzverlauf

Das Schutzverlauf-Widget gibt den Prozentsatz unsicherer Inhalte während der aktuellen Zeitspanne im Vergleich zum Durchschnitt und der vorherigen Periode an. Die Verlaufsinformationen vermitteln jederzeit, ob der Sicherheitsstatus der Firma auf dem gleichen Niveau bleibt oder ob es einen plötzlichen Anstieg unsicherer Inhalte gibt, der mit einem Angriff zusammenhängen könnte.

2.3.8. Analytics

F-Secure Cloud Protection für Microsoft Office 365 bietet eine lückenlose Transparenz für die Nutzung von MS O 365 Exchange. Alle Sicherheitswarnungen für verdächtige Inhalte, die in den Postfächern auftauchen, sind im Portal per Tabellenansicht zugänglich. Die Tabelle lässt sich leicht durchsuchen und nach verschiedenen Kriterien sortieren.

Viele IT-Abteilungen wissen nicht, welche Art von Inhalten ihre User über MS O 365 Exchange senden oder empfangen. Solche Informationen wären aber hilfreich, um Dateien oder URLs zu erkennen, welche für Angriffe verwendet werden können und nicht über MS O 365 ausgetauscht werden sollten.

Außerdem hilft ein besseres Verständnis der internen Kundenbedürfnisse und Anwendungsfälle den Administratoren, ihr Unternehmen effektiver zu betreuen. Mit leistungsstarken Suchfunktionen können sie und IT-Sicherheitsabteilungen inhaltsbasierte Angriffe extrem schnell untersuchen.

2.3.9. Richtlinienverwaltung

F-Secure Cloud Protection für Microsoft Office 365 bietet Richtlinien zur Definition der Sicherheitseinstellungen für die analysierten Inhalte in MS-O-365-Exchange-Elementen. Eine Richtlinie ist eine Sammlung von Einstellungen und Regeln, die festlegen, wie der Dienst die Postfächer schützt und welche Maßnahmen ergriffen werden, wenn eine Sicherheitserkennung auftritt.

Administratoren können die F-Secure-Standardrichtlinie verwenden, um bei der Konfiguration maximalen Schutz zu erreichen. Sie können alternativ die Standardrichtlinie kopieren, um die Sicherheitseinstellungen den Firmenanforderungen anzupassen, und diese dann zur Standardrichtlinie erheben.

2.3.10. Quarantänemanagement

F-Secure Cloud Protection für Microsoft Office 365 ermöglicht es zudem, ein Exchange-Element auf Basis der Schädlichkeit gefundener Dateien und URLs unter Quarantäne zu stellen. Im Quarantänebereich im Verwaltungsportal kann man isolierte Elemente anzeigen, freigeben oder löschen. Der Administrator kann verschiedene Sortier- und Suchkriterien verwenden, während er die Liste der unter Quarantäne gestellten Elemente bearbeitet.

2.3.11. Berichterstattung

F-Secure Cloud Protection für Microsoft Office 365 wartet mit umfangreichen Berichtsfunktionen auf, mit denen Administratoren jederzeit in einem leicht zugänglichen Format den Sicherheitsstatus der geschützten Umgebung auswerten können.

DerAdministrator legt den Inhalt und den Zeitplan (täglich, wöchentlich, monatlich) der automatisch zu erstellenden Berichte fest, die sich dann im Portal herunterladen lassen. Darüber hinaus können Verantwortliche eine Zusammenfassung des Sicherheitsstatus als Nachricht verfassen, die dem Anfang des generierten Berichts beigefügt wird.

3. F-SECURE SECURITY CLOUD

Die Security Cloud von F-Secure ist ein cloudbasiertes Bedrohungsanalysesystem. Es besteht aus einer ständig wachsenden und sich weiterentwickelnden Wissensdatenbank über digitale Gefahren, die aus Daten des Client-Systems und automatisierten Analysediensten gespeist wird. Die Infrastruktur der Security Cloud wird auf Servern in mehreren Amazon-Web-Service-Rechenzentren auf der ganzen Welt gehostet. Die Security Cloud ist ein System mit sehr hohem Volumen, das täglich über acht Milliarden Anfragen erhält.

Wir sammeln nur die Mindestmenge an Kundendaten für unsere Services. Jedes übertragene Bit muss aus Sicht der Bedrohungsprävention gerechtfertigt sein, und Daten werden nie für mutmaßliche zukünftige Zwecke gesammelt. Mit den Standardeinstellungen hortet die Security Cloud keine IP-Adressen, Dateien oder andere private Informationen. Kunden können F-Secure die Erlaubnis erteilen, verdächtige ausführbare Dateien und/oder nicht ausführbare Dateien zu speichern.

Durch die Auswertung der kombinierten Metadaten mit Informationen aus firmeneigenen Datenbanken und verschiedenen anderen Quellen liefern die automatisierten Analysesysteme umfassende und aktuelle Risikobewertungen. Sie blockieren sofort alle Bedrohungen, die zuvor von einem anderen mit der Security Cloud verbundenen Service oder Gerät aufgedeckt wurden.

Die Security Cloud ermöglicht es den Analysten von F-Secure Labs zudem, als Ergänzung zu den automatisierten Systemen und der On-Host-Scantechnologie wichtige menschliche Informationen und Beurteilungen zu liefern. Zusätzlich zur Erstellung und Pflege der Regeln, die den Datenbanken und automatisierten Analysesystemen zugrunde liegen, überwachen die Analysten aktiv die neuesten Gefahren. Sie untersuchen Malware-Merkmale und Verhaltensmuster, um die effektivsten Wege zur Identifizierung feindlicher Programme zu finden.

Die folgende Tabelle dokumentiert unsere Datenschutzprinzipien im Detail:

Minimierung technischer Daten	Die Security Cloud von F-Secure setzt eine mehrstufige Inhaltsanalyse ein. Dateidaten werden nicht an die Security Cloud gesendet – es sei denn, sie sind für den Schutz unerlässlich und der Kunde hat seine Erlaubnis erteilt.
Keine Übermittlung von persönlichen Daten	Keine Informationen darüber, wer die analysierten Dateien oder URLs veröffentlicht oder auf sie zugreift. Plus keine Infos, von wo aus sie an die Security Cloud gesendet werden.
Kein Vertrauen ins Netzwerk	Alle Metadaten, Dateien und anderen Inhalte werden entweder über HTTPS oder separat verschlüsselt und signiert über HTTP sicher in die Security Cloud übertragen.

Prinzipien der Security Cloud:

Secure by Design	Ein System ist nie sicher – es sei denn, es wurde so konzipiert, dass es sicher ist. Sicherheit kann nicht nachträglich verankert werden. Bei der Entwicklung der Security Cloud und der mit ihr verbundenen Komponenten hatten wir das im Hinterkopf.
Verschlüsselter Netzwerkverkehr	Daten werden nie im Plain Text über das Internet übertragen. Zudem kommt eine Verschlüsselung zum Einsatz, um die Integrität verschiedener Objekte zu gewährleisten. F-Secure verwendet eine Mischung aus allgemein verfügbaren kryptografischen Bibliotheken und Protokollen sowie angepasstem kryptografischem Code.
Getrennte Malware-Umgebungen	Wir verfügen über mehr als 20 Jahre Erfahrung im Umgang mit bösartiger Software. Die gesamte Malware-Handhabung erfolgt in Netzwerken, die vom Internet und anderen F-Secure-Netzwerken isoliert sind. Speicher- und Testnetzwerke sind voneinander separiert, Dateien werden mit streng kontrollierten Methoden übertragen.
Professionelle Überwachung	F-Secure-Mitarbeiter überwachen alle kritischen Security-Cloud-Systeme. Alle Systeme, die Malware speichern oder testen, hostet die F-Secure Corporation.
Kontrollierter Zugang	Nur eine begrenzte Anzahl von F-Secure-Mitarbeitern bekommt Zugang zu den kritischen Systemen der Security Cloud. Dieser Zugang erfolgt nur nach einem dokumentierten und kontrollierten Prozess, der auch widerrufen werden kann.
Offener Ansatz	Das grundlegendste Prinzip in der gesamten Sicherheitsarbeit: Offenheit und Bescheidenheit. Wir haben viel Mühe in die Sicherung der Security Cloud investiert, aber die Arbeit geht immer weiter. Ein sicheres System kann nur durch die Förderung einer offenen Einstellung aufrechterhalten werden, in der Systemprobleme zeitnah gemeldet, analysiert und behoben werden. Zu dieser Haltung gehört eine öffentliche Transparenz, sollten wir auf Vorfälle stoßen, die die Sicherheit der Kunden gefährden.

Erfahren Sie mehr über die Security Cloud von F-Secure in unserem Security Cloud Whitepaper und der Datenschutzrichtlinie für Security Cloud.

3.1. Threat Intelligence Service

Die Nutzung von Echtzeit-Bedrohungsinformationen, die von Zigmillionen Sensoren gesammelt werden, ermöglicht die Erkennung neuer und aufkommender Gefahren innerhalb weniger Minuten nach ihrem Auftreten. So können wir eine außergewöhnliche Sicherheit vor der sich ständig weiterentwickelnden Bedrohungslandschaft gewährleisten. Unser Threat Intelligence Service ermöglicht es F-Secure Cloud Protection, Objekte wie Dateien und URLs einzuschätzen. Dateien werden verifiziert, indem der kryptografische Hash SHA-1 des Objekts berechnet und an den Reputationsservice gesendet wird.

3.2. Multi-Engine-Antivirensoftware

Die Multi-Engine-Antivirensoftware nutzt mehrere Sicherheitsebenen, um Exploits und unbekannte Malware zu erkennen, die bei gezielten Angriffen zum Einsatz kommen. Das System kombiniert Verhaltensanalysen mit heuristischen und maschinellen Erkennungsfunktionen, die es ihm ermöglichen, spezifische Malware, Familien von Malware mit ähnlichen Merkmalen und eine breite Palette bösartiger physischer Merkmale und Muster zu identifizieren. Die Ergebnisse dieser Analyse führen eventuell dazu, dass die Datei als verdächtig markiert und zur weiteren Verarbeitung an die Cloud-Sandbox weitergeleitet wird.

3.3. Cloud-Sandbox

Die Cloud-Sandbox führt erkannte Dateien in mehreren virtuellen Umgebungen aus und analysiert ihr Verhalten. Erscheint die Datei verdächtig, werden Informationen an die Multi-Engine-Antivirensoftware und an den Threat Intelligence Service gesendet, wo die Gefahr bei der nächsten Überprüfung blockiert wird.

ÜBER F-SECURE

Niemand hat einen besseren Einblick in echte Cyber-Angriffe als F-Secure. Wir schließen die Lücke zwischen Erkennung und Reaktion. Zu diesem Zweck nutzen wir die konkurrenzlosen Informationen über Bedrohungen von Hunderten der besten technischen Berater unserer Branche, Millionen von Geräten, die unsere preisgekrönte Software nutzen, sowie fortlaufenden Innovationen im Bereich Künstliche Intelligenz. Führende Banken, Fluggesellschaften und Unternehmen vertrauen auf unser Engagement bei der Bekämpfung der gefährlichsten Bedrohungen der Welt.

Zusammen mit unserem Netzwerk an Top-Channel-Partnern und über 200 Serviceanbietern ist es unsere Mission, all unseren Kunden maßgeschneiderte unternehmensfähige Cyber-Sicherheit zur Verfügung zu stellen. F-Secure wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd gelistet.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

F-Secure