Trend Micro

SMART PROTECTION NETWORK SMART FEEDBACK

Durch Ihre Teilnahme am Smart Feedback Programm kann das Trend Micro™ Smart Protection Network™ Informationen über mögliche Bedrohungen für Ihre Netzwerkumgebung erfassen. Dieser Überblick erläutert die Vorteile der Verwendung von Smart Feedback.

WAS IST DAS SMART PROTECTION NETWORK?

Mithilfe des Smart Protection Network können Trend Micro Kunden mögliche Bedrohungen sofort analysieren. Es beinhaltet eine kontinuierliche und schnelle wechselseitige Kommunikation zwischen installierten Trend Micro Sicherheitslösungen und Trend Micro Zentren für Bedrohungsforschung.

Das Smart Protection Network nutzt den Vorteil von Big-Data-Analysen, um neue Bedrohungen mithilfe von weltweit erfassten Daten zu identifizieren. **Smart Feedback**, eine entscheidende Komponente des Smart Protection Network, stellt sicher, dass mögliche Bedrohungen in Ihrer individuellen Netzwerkumgebung schnell erkannt und abgewehrt werden können.

WARUM SOLLTEN SIE SMART FEEDBACK AKTIVIEREN?

In der Bedrohungslandschaft von heute lässt sich ein deutlicher Trend erkennen: Während Bedrohungen bisher gegen eine breite Masse von Einzelpersonen und Unternehmen gerichtet waren, beobachten wir gegenwärtig vermehrt konzentrierte und gezielte Angriffe. Unsere Kunden haben daher heute mit Angriffen zu tun, die sich konkret gegen ihr Unternehmen richten. Trend Micro muss Informationen über potenzielle Bedrohungen also direkt von jedem Kunden erfassen. Eine Aktivierung des Smart Feedback (über die Lösungsoberfläche) trägt unterstützend dazu bei, dass Trend Micro Big-Data-Analysen effektiv nutzen kann, um diese neuen Bedrohungen zu erkennen und abzuwehren.

Jeder Kunde, der Daten zu möglichen Bedrohungen mit Trend Micro austauscht, verbessert nicht nur den eigenen Schutz, sondern auch den der Allgemeinheit. Mit Ihrer Hilfe kann Trend Micro innerhalb von Branchen, Regionen oder anderen Gruppierungen verborgene Trends erkennen, die sich aus den gemeinsam verwendeten Daten ergeben.

Sie haben Bedenken hinsichtlich des Datenschutzes bei der Nutzung von Smart Feedback? Dann lesen Sie bitte weiter.

GRUNDSÄTZE UND RICHTLINIEN

Trend Micro hat das Smart Protection Network nach folgenden Grundsätzen entwickelt und implementiert:

- **Anonymisierte Daten:** Das Smart Protection Network speichert ausschließlich anonymisierte Daten und vermeidet die Erfassung personenbezogener Daten (Personally Identifiable Information, PII). Weitere Informationen erhalten Sie im Abschnitt „Datenanonymisierung".
- **Datenschutz und Privatsphäre unserer Kunden hat höchste Priorität:** Trend Micro speichert alle erfassten Daten oder Informationen auf sichere Weise. Weitere Informationen erhalten Sie im Abschnitt „Datenschutz".
- **Nutzung zur Optimierung von Sicherheitslösungen:** Trend Micro nutzt die erfassten Daten im Rahmen des Smart Feedback Programms, um den Schutz von Trend Micro Kunden kontinuierlich zu verbessern. Trend Micro verwendet diese Daten nicht für gezielte Werbung.
- **Branchenspezifische Daten:** Trend Micro erfasst Kundenfeedback nach Branche, um spezifische Probleme schnell zu erkennen und Lösungen für Bedrohungen bereitzustellen, die sich gegen einen bestimmten Unternehmenstyp richten.
- **An- oder Abmeldung jederzeit möglich:** Sie können Smart Feedback jederzeit über die Administrationsoptionen in Ihrer Trend Micro Software aktivieren bzw. deaktivieren.
- **Löschung der von Ihnen gesendeten Daten auf Anfrage:** Sie können jederzeit beantragen, dass die gesendeten Daten gelöscht werden. Wenden Sie sich hierzu an Trend Micro unter DeleteMyData@trendmicro.com.

AUF WELCHE WEISE NUTZT TREND MICRO DIE ERFASSTEN DATEN?

Trend Micro nutzt Daten aus dem Smart Protection Network, um Erkenntnisse über Bedrohungsverhalten und Trends zu gewinnen und damit die Wirksamkeit von Sicherheitslösungen kontinuierlich zu verbessern.

- **Schnellere Reaktionen auf Bedrohungen:** Das Smart Protection Network stellt Ihnen den neuesten Schutz in Echtzeit bereit. Im Vergleich zu herkömmlichen Methoden mit Signatur-Updates reduziert dieser Ansatz Ihr Zeitfenster für vorhandene Sicherheitslücken von (möglicherweise mehreren) Tagen auf wenige Minuten. Dank des Smart Feedback Programms kann Trend Micro mitverfolgen, wie sich Cyberangriffe verändern und weiterentwickeln.
- **Starke Abwehr gezielter Angriffe:** Cyberkriminelle rücken von eher breitgestreuten Angriffen ab und nehmen zunehmend individuelle Ziele ins Visier. Smart Feedback von Kunden ermöglicht es uns, neue Angriffsquellen und -methoden zu identifizieren.
- **Aufdeckung verborgener Bedrohungen:** Mithilfe weltweit erfasster Daten kann Trend Micro Big-Data-Analysen nutzen, um wichtige Beziehungen während eines Angriffs zu erkennen und Licht auf sorgfältig verborgene Bedrohungen zu werfen. Darüber hinaus tragen diese Daten dazu bei, dass Trend Micro Zero-Day-Schwachstellen erkennen und einen entsprechend aktualisierten Schutz sehr viel schneller bereitstellen kann.
- **Bessere Ergebnisse:** Diese in Echtzeit durch das Smart Protection Network erfassten Statistiken verbessern die Gesamtqualität und -leistung der Trend Micro Lösungen und Services.

DATENANONYMISIERUNG

Trend Micro nutzt das Smart Feedback Programm, um Informationen über potenzielle Sicherheitsbedrohungen auf Ihrem Computer oder in Ihrem Netzwerk zu Analysezwecken zu erfassen. Folgende Datentypen werden erfasst:

- Verdächtige ausführbare Dateien
- Adressen, Domains und IP-Adressen besuchter Websites
- Informationen über laufende Anwendungen, einschließlich Datei-, Prozess- und Registry-Daten

Das Smart Protection Network wurde von Trend Micro so konzipiert, dass die Erfassung personenbezogener Daten möglichst vermieden wird. Durch das Ausklammern spezifischer personenbezogener Daten und das ausschließliche Speichern anonymer Verhaltensprofile gelingt es Trend Micro, Ihre Privatsphäre zu wahren und gleichzeitig neue Bedrohungen zu entdecken.

Der Anonymisierungsprozess beinhaltet verschiedene unterscheidbare Ebenen, einschließlich:

- **Anonymisierte Dateipfade:** Die Metadaten ausführbarer Dateien enthalten möglicherweise einen Dateipfad, der personenbezogene Daten umfasst. Im folgenden Beispiel sehen Sie, wie Trend Micro diesen potenziell vertraulichen Teil des Dateipfads verbirgt:

  C:\Benutzer**John**\Desktop\setup.exe
  wird zu:
  C:\Benutzer\%**BENUTZERPROFIL**%\Desktop\setup.exe

- **Sicherheitsdaten aus verdächtigen E-Mails:** Smart Feedback erfasst nur Informationen aus E-Mail-Nachrichten, die verdächtige Merkmale aufweisen. Diese Informationen können jedoch personenbezogene Daten enthalten. Alle erfassten Daten werden daher vor der Übertragung vom Computer verschlüsselt. Trend Micro speichert diese Daten auf sichere Weise und nutzt sie ausschließlich, um potenzielle neue Bedrohungen zu entdecken.

DATENSCHUTZ

Bei Trend Micro hat die Sicherheit von Kundendaten oberste Priorität. Neben Datenanonymisierung nutzt das Smart Protection Network weitere Maßnahmen, um Daten zu schützen.

Beachten Sie bitte, dass Trend Micro personenbezogene Daten, die zu geschäftlichen Zwecken erforderlich sind (z. B. für das Lizenzmanagement oder technischen Support), in separaten Systemen getrennt vom Smart Protection Network speichert. Daten dieser Art sind daher nicht Gegenstand dieses Dokuments.

- **Daten während der Übertragung**
  Das Smart Protection Network verschlüsselt alle Daten vor der Übertragung an Trend Micro unter Verwendung branchenüblicher Verschlüsselungstechnologien in Kombination mit zusätzlicher Zielserver-Authentifizierung.

- **Zugriffssteuerung und Auditing**
  Trend Micro befolgt beim Schutz von Daten aus dem Smart Protection Network strenge Verfahren. Nur Trend Micro Forschungsteams aus speziellen Abteilungen haben Zugriff auf diese Informationen, wobei die Zugriffsrechte eine explizite Genehmigung erfordern, die durch Trend Micro regelmäßig überprüft wird. Zu Auditierungszwecken verwaltet Trend Micro umfassende Datensätze mit entsprechenden Zugriffsrechten und Informationen zur Datenvernichtung.

- **Datenaufbewahrung und -löschung**
  Trend Micro speichert Daten bei Bedarf, um Analysen durchzuführen und das Smart Protection Network kontinuierlich zu aktualisieren. Sie haben jedoch jederzeit die Möglichkeit, Trend Micro zum Löschen der Daten aufzufordern, die von Ihren Computern und Netzwerken stammen.

  Wenn Sie die Löschung anonymer Daten aus dem Smart Protection Network beantragen, müssen Sie Informationen zur Identifizierung der betreffenden Daten bereitstellen, damit Trend Micro die richtigen Datensätze entfernen kann. In einigen Fällen können daher möglicherweise nicht alle von Ihnen gesendeten Daten entfernt werden.

ÜBERTRAGENE DATENTYPEN

PRODUKTLIZENZDATEN

Dieser Abschnitt beschreibt die Daten, die eine Identifizierung Ihrer Person zu Lizenz- und Supportzwecken ermöglichen. Diese Art von Daten werden immer, auch bei deaktiviertem Smart Feedback, an Trend Micro übermittelt.

Datenelement	Zweck	Hinweise
Software-Lizenzschlüssel	Stellt die Gültigkeit Ihrer Softwarelizenz sicher	Diese Daten werden von Trend Micro sicher verwaltet. Der Zugriff ist auf eine Gruppe autorisierter Mitarbeiter beschränkt.

DATEN AUS VERDÄCHTIGEN E-MAILS

Dieser Abschnitt beschreibt die Daten, die bei aktiviertem Smart Feedback aus E-Mail-Nachrichten mit verdächtigen Merkmalen erfasst werden. Trend Micro erfasst keine Daten aus anderen Nachrichten.

Datenelement	Zweck	Hinweise
• E-Mail-Adresse von Absender und Empfänger • E-Mail-Betreff • Dateiname von Anhängen (falls vorhanden) • Telefonnummer (falls vorhanden)	Verbessert Erkennungsraten bei Phishing-E-Mails	Trend Micro überprüft nur potenziell gefährliche Nachrichten und verschlüsselt alle Inhalte vor der Übertragung von Daten.

GRUNDLEGENDE ANONYME DATEN

In diesem Abschnitt sind alle Daten aufgeführt, die bei aktiviertem Smart Feedback durch Trend Micro Software und Services erfasst werden. Trend Micro kann diese anonymisierten Daten keiner bestimmten Person zuordnen.

Datenelement	Zweck	Hinweise
Zufällige, einzigartige Geräte-ID	Identifiziert jede Instanz eines Trend Micro Geräts oder einer Trend Micro Installation, damit Trend Micro Services oder technischen Support bereitstellen kann.	Trend Micro erzeugt diese ID nach dem Zufallsprinzip während des Produkt-Setups. Die ID lässt keine Rückschlüsse auf eine bestimmte Person zu.
Produktinformationen	Gibt an, welches Trend Micro Produkt die Feedback-Daten gesendet hat.	
Betriebssysteminformationen	Unterstützt die Entwicklung von Produktfunktionsgruppen und die Priorisierung von Wartungs-anforderungen zu statistischen Zwecken	
Öffentliche IP-Adresse	Bietet Standortdaten auf Stadtebene	Zur Bestimmung der Produkt-verteilung
Daten zur PC- bzw. mobilen Umgebung	Unterstützt die Analyse von Cloud-Daten und Premium Services	
Metadaten ausführbarer Dateien	Trägt zur Identifizierung bösartiger Dateien bei	Daten beinhalten möglicherweise Dateipfade
URLs, Domänen und IP-Adressen besuchter Websites	Stellt Schutz auf Endpunkten nahezu in Echtzeit bereit	
Metadaten des von Gateway-Produkten verwalteten Clients oder Geräts	Zur Bereitstellung erweiterter Funktionen	
Branchenspezifische Daten	Unterstützt die Bereitstellung von individuellem Schutz vor branchen-spezifischen Bedrohungen	Kunde muss nach Aktivierung des Smart Feedback eine Option aus Dropdown-Liste auswählen

ERWEITERTE ANONYME DATEN

Bei aktiviertem Smart Feedback erfassen Trend Micro Software und Services detailliertere (aber dennoch anonyme) Daten zur Erkennung potenzieller Bedrohungsaktivitäten.

Datenelement	Zweck	Hinweise
Anwendungsverhalten in Sandboxes	Ständige Rückmeldung von installierten Produkten, um deren Wirksamkeit zu überprüfen	Diese Ergebnisse können nur von Angeboten mit Sandboxing-Funktion gesendet werden.
Daten aus verdächtigen E-Mails	Verbessert die Erkennung von Spam- und Phishing-E-Mails	Trend Micro überprüft nur potenziell gefährliche Nachrichten und verschlüsselt alle Inhalte vor der Übertragung von Daten.
Verdächtige ausführbare Dateien	Verbessert die Erkennungsfunktionen von Trend Micro Produkten	
Daten zu erkannten bösartigen Dateien	Verbessert die Erkennungsfunktion und Leistung von Trend Micro Produkten	
Daten zu erkannten bösartigen Prozessen	Verbessert die Erkennungsfunktion und Leistung von Trend Micro Produkten	
Daten zu erkannten bösartigen Netzwerkverbindungen	Verbessert die Erkennungsfunktion und Leistung von Trend Micro Produkten	