A1 Telekom Austria AG Lassallestraße 9, 1020 Wien

Offensity Security Monitoring & Reporting

Servicebeschreibung

Version: 3.0

Datum: 18.02.2019

Inhaltsverzeichnis

1 Allgemeines

Diese Servicebeschreibung gilt ab 18.02.2019. Sie erläutert die Ausprägung aller Anwendungen von Offensity Security Monitoring (kurz „Offensity"), die Ihnen als Kunde von A1 Telekom Austria AG (kurz „A1") angeboten und bereitgestellt werden. Sofern hier nicht Abweichendes geregelt wird, kommen die Allgemeinen Geschäftsbedingungen für Cloud und Software Solutions der A1 Telekom Austria AG zur Anwendung.

Alle Offensity Anwendungen sind cloudbasierte Services, die ortsunabhängig genutzt werden können. Die Kunden erhalten die notwendigen Zugangsdaten für die Dauer des gewählten Abonnements (monatlich, jährlich).

Kunde für das Service Offensity kann nur ein Unternehmer im Sinne des § 1 des Konsumentenschutzgesetzes (KSchG) sein.

2 Anwendungen

Offensity hilft Unternehmen dabei, die zur Sicherheit ihrer extern erreichbaren IT-Systeme (wie DNS-, Mail- und Webserver, Mailinglisten) technische Maßnahmen nach dem Stand der Technik ergreifen wollen, laufend Schwachstellen zu erkennen und

versteckte Webseiten im „Deep Web" (auch „Verstecktes Web") auf Ihre unfreiwillig veröffentlichten Datensätze hin zu überwachen. Eine einheitliche Erfassung aller identifizierten Risiken sowie lösungsorientierte Reports reduzieren die Reaktionszeit des Kunden und ermöglichen eine Dokumentation und Priorisierung der zu setzenden Maßnahmen.

A1 übernimmt keinerlei Verantwortung dafür, dass alle vorhandenen Schwachstellen erkannt werden. Abhängig von den gewählten Konfigurationen, ist es beispielsweise immer möglich, einzelne Systeme oder Schwachstellen zu übersehen.

Offensity beinhaltet folgende Anwendungen: Domain-basiertes Asset Discovery, Schwachstellen-Scans und Risikobewertung, „Deep-Web"-Überwachung, und Lösungsorientierte Reports. Die durch Offensity erkannten Schwachstellen und Datensätze werden vertraulich behandelt.

2.1 Domain-basiertes Asset Discovery

Auf Basis von Domain-Namen des Kunden (z.B. „example.com") werden dazugehörende, extern erreichbare IT-Systeme erhoben. Dies umfasst beispielsweise DNS- und Mailserver sowie Subdomains. Diese Erhebung erfolgt über öffentliche und teilöffentliche Quellen.

2.1.1 Domain Control Validation

Die Kunden können bei Aktivierung der Domain aktuell zwischen folgenden drei dem „Stand der Technik" entsprechenden technischen Methoden wählen, mit denen Offensity die Domain-Ownership verifiziert:

- **E-Mail-basierte Domain Control Validation**: Wenn die Bestellung aufgegeben wird, wird eine E-Mail-Adresse aus einer Liste mit akzeptablen Optionen ausgewählt. An diese Adresse wird eine E-Mail gesendet, die einen eindeutigen Validierungscode enthält. Die E-Mail sollte von einer Person empfangen werden, die die Kontrolle über die Domain innehat. Die Liste der zulässigen E-Mail-Adressen für eine bestimmte Domain lautet beispielsweise admin@, administrator@, hostmaster@, postmaster@ oder es handelt sich dabei um eine beliebige E-Mail-Adresse für Administrator, Registrant, Tech oder Zone, die im WHOIS-Verzeichnis[1] aufscheint.
- **DNS-based Domain Control Validation**: Der Kunde muss einen vordefinierten Textcode als so genannten DNS-Texteintrag in seine DNS-Verwaltungskonsole hochladen.

[1] Das WHOIS-Verzeichnis ist eine öffentliche Liste von Domainamen und Kontaktdaten der mit ihnen verknüpften Personen oder Organisationen.

- **HTTP-based Domain Control Validation**: Der Kunde muss eine Authentifizierungsdatei in den Stammordner seiner Website hochladen.

2.2 Schwachstellen-Scans und Risikobewertung

Die Systeme werden aus dem Internet netzseitig mit Hilfe von Security-Scannern und automatisierten Analysen untersucht, um Informationen oder Hinweise zu erhalten, die ein Angreifer für die Vorbereitung und Durchführung von virtuellen Einbrüchen nutzen kann. Die eingesetzten Werkzeuge überprüfen aktuell bekannte Schwachstellen von Netzwerkkomponenten, Betriebssystemen, Applikationen und Protokollen, soweit sie aus dem Internet nachweisbar sind. Diese werden im Rahmen einer automatisierten Risikoanalyse bewertet. Der Risikostatus wird dokumentiert und kann jederzeit mit vergangenen Ergebnissen verglichen werden. Bei Bekanntwerden neuer Schwachstellen wird – abhängig von technischer Möglichkeit, Umsetzbarkeit, Risikopotenzial und Relevanz – die Kundeninfrastruktur auf Anfälligkeit überprüft.

Der Kunde hat dafür zu sorgen, dass jene Systeme, die für Schwachstellen-Scans verwendet werden, von dynamischen Sicherheitseinschränkungen (wie z.B. Web Application Firewalls, fail2ban, etc.) ausgenommen werden. Eine Ausnahme von statischen Sicherheitsmaßnahmen (wie etwa Packet Filtering Firewall) ist möglich, wird seitens A1 aber nicht empfohlen.

Die Quellsysteme und deren IP-Adressbereiche, die für Schwachstellen-Scans verwendet werden, werden dem Kunden auf Anfrage mitgeteilt.

Von Offensity wird pro Subdomain max. eine dahinterliegende IPv4-Adresse und eine weitere dahinterliegende IPv6-Adresse gescannt.

2.2.1 Permission To Attack

Die Schwachstellen Scans („Security-Scans") können „intrusiv" und „nicht-intrusiv" sein.

- **Intrusive Security-Scans** sind Scans, die technische oder organisatorische Schutzmaßnahmen umgehen können. Diese Scans bedürfen einer rechtlich verbindlichen Zustimmung durch den Kunden bzw. einen Administrator, dass die aktivierten Subdomains unter jeder Domain (inkl. den dahinterliegenden IP-Adressen) durch Offensity auf Schwachstellen gescannt werden dürfen (sog. „Permission To Attack"). Ohne eine solche Zustimmung können diese Scans illegal sein.
- **Nicht-intrusive Security-Scans** sind Scans, die keine technischen oder organisatorischen Schutzmaßnahmen umgehen, um auf das Vorhandensein von Schwachstellen zu schließen. Dies umfasst etwa das

Herausfinden von Software-Versionen. Es ist in der Regel keine Zustimmung des System-Besitzers notwendig.

A1 weist darauf hin, dass die Durchführung von Security-Scans und Penetrationstests die Verfügbarkeit und Integrität der Zielsysteme beeinträchtigen kann. Es ist möglich, dass der ordnungsgemäße Betrieb nur durch manuellen Zugriff auf das Zielsystem wiederhergestellt werden kann. Dies bedeutet beispielsweise, dass die Webseite auf dem Zielsystem nicht mehr erreichbar sein könnte, bzw. dass Registrierungen, Anmeldungen oder Bestellungen mit unrichtigen Daten durchgeführt werden könnten. Dafür ist die Haftung von A1 ausgeschlossen.

Jede identifizierte Subdomain muss durch den Kunden explizit freigeschalten werden, damit sie gescannt wird. Mit dem Freischalten der Subdomain gibt der Kunde verbindlich bekannt, dass er die Befugnis hat, dahinter liegende IP-Adressen attackieren zu lassen. Bei Änderung der DNS-Einträge auf weitere oder andere IP-Adressen ist der Kunde dazu verpflichtet, die Subdomain zu deaktivieren. Bei Nicht-Deaktivierung darf Offensity davon ausgehen, dass der Kunde die Befugnis hat, auch die aktualisierten IP-Adressen zu attackieren.

Alle Fragen betreffend Rechte an den Domains (z.B. Registrierung, Innehabung, Sperre, Kauf, Miete, Pacht, Sharing, Urheberrechte, Namensrecht, Markenrecht usw.) und allenfalls daraus resultierende Konflikte wird der Kunde im eigenen Bereich abschließend lösen.

A1 haftet nur bei Vorsatz oder grober Fahrlässigkeit. Die Haftung für entgangenen Gewinn, ausgebliebene Einsparungen, Zinsverluste, mittelbare und Folgeschäden, ideelle Schäden, sowie Schäden aus Ansprüchen Dritter, sowie für verlorengegangene oder veränderte Daten ist ausgeschlossen. Der Kunde hält weiters die A1 hinsichtlich sämtlicher von Dritter Seite erhobener Ansprüche in vollem Umfang schad- und klaglos.

2.2.2 Kundeninformation zu Scans

Wenn ein Scan auf die http-Services der Kunden gestartet wird, wird nach dem Auslesen der URLs aus der Datenbank automatisch ein GET-Request zu den einzelnen URLs abgeschickt mit einem Link, über den grundlegende Infos zu Offensity abgerufen werden können. Wenn es weitere Anliegen gibt, ist auf der verlinkten Website eine Kontakt-Adresse veröffentlicht.

2.3 „Deep-Web"-Überwachung

Unfreiwillig veröffentlichte Datensätze dritter Plattformen können zu Sicherheitsproblemen führen, da etwa E-Mail-Adressen und Zugangsdaten von den Nutzern dieser Plattformen in fremde Hände geraten. Offensity überwacht das „Deep Web" (auch „Verstecktes Web"), um veröffentlichte Daten aufzuspüren. Gefundene Datensätze werden auf Basis der Kunden-Domains selektiert und verifiziert, um Kunden über veröffentlichte Datensätze zeitnah zu informieren.

Offensity gleicht Domains und IP-Adressen der Kunden mit öffentlichen und teilöffentlichen Block- und Blacklisten ab, um eine Servicebeeinträchtigung der Kundendienste möglichst frühzeitig zu erkennen. Einträge auf diesen Listen können auch auf Missbrauch oder Kompromittierung der Kundensysteme hinweisen.

2.4 Lösungsorientierte Reports

Die Ergebnisse der laufenden Scans werden in Form eines schriftlichen Reports zur Verfügung gestellt. Es wird eine Kategorisierung der ggf. gefundenen Schwachstellen vorgenommen, die Schwachstelle wird beschrieben, ggf. werden weiterführende Informationen und Hinweise zur Behebung der Schwachstelle dargelegt. Der Bericht wird in englischer Sprache verfasst.

3 Leistungsumfang

Die Leistung von Offensity beinhaltet folgende Lieferobjekte:

- Offensity Security Monitoring inkl. „2.1 Domain-basiertes Asset Discovery", „2.2 Schwachstellen-Scans und Risikobewertung", „2.3 ‚Deep-Web'-Überwachung"
- Einen Report pro Quartal (siehe „2.4 Lösungsorientierte Reports")

4 Datenarten

Im Rahmen des Services Offensity werden folgende Datenarten verarbeitet:

- Personen-Stammdaten
  - E-Mail-Adresse
  - Passwort
  - Firmenname
  - Vorname

  - Zuname
  - Telefonnummer (optional aber empfohlen)
  - Straße + Hausnummer
  - PLZ
  - Ort
  - Land
- Domainnamen (inkl. Subdomains und IP-Adressen)
- Zahlungsdaten