

Securepoint Awareness PLUS

- Leistungsbeschreibung -

Datum: 28.04.2022, Version: 2.0, Autor: Eric Kaiser, Anpassung: Stefanie Hein-Heine

LEISTUNGSELEMENTE	2
PREISE	2
VERTRAGSLAUFZEIT	2
ABRECHNUNG	2
WEITERENTWICKLUNG DES ANGEBOTES	2
ALLGEMEINES	2
NUTZUNGS- UND URHEBERRECHTE	3
GEWÄHRLEISTUNG	4
SERVICE LEVEL AGREEMENT (SLA)	4
Geltungsbereich	4
Voraussetzungen und Mitwirkungspflichten für die Nutzung der Leistungen	5
Allgemeine Voraussetzungen und Mitwirkungspflichten	5
Spezielle Voraussetzungen und Mitwirkungspflichten	5
Leistungsbausteine	5
Phishing-Simulation	5
Zugriff über Lernplattform	6
Securepoint Manager	6
Leistungsumfang einzelner Awareness-Pakete	6
VERFÜGBARKEIT DER DIENSTE	7
Generelle Verfügbarkeit	7
Ausnahmen von der Verfügbarkeit	8
Unterschreitung der Verfügbarkeit	8

Leistungselemente

Securepoint Awareness PLUS setzt sich aus zwei Bausteinen zusammen (im Folgenden „Leistungsbausteine“). Hierzu zählen Phishing-Simulationen und die Bereitstellung von darauf aufbauenden E-Learning-Modulen. Teilweise werden die Leistungsbausteine webbasiert zur Verfügung gestellt.

Preise

Sämtliche Preise entnehmen Sie bitte der aktuellen Preisliste.

Es wird die Menge aller Nutzer aus allen dem Partner / Reseller zugeordneten Lizenzen zum von Securepoint festgelegten Stichtag jeden Monat erhoben und zum in der aktuellen Preisliste genannten Preis abgerechnet.

Ein Nutzer ist ein auf der Awareness Plattform (manager.awareness.securepoint.cloud) angelegter und aktiver Nutzer.

Vertragslaufzeit

Je Endkunde erzeugt der Vertragspartner eine eigene Lizenz. Diese Lizenz hat eine Mindestvertragslaufzeit von 12 Monaten nach dem Anlegen des ersten Benutzers innerhalb dieser Lizenz. Der Vertrag verlängert sich automatisch um weitere 12 Monate, sofern er nicht mit einer Frist von 4 Wochen zum Ende der Vertragslaufzeit gekündigt wird.

Abrechnung

Abrechnungszeitraum ist monatlich. Die Berechnung erfolgt monatlich rückwirkend. Angefangene Monate werden als volle Monate berechnet. Die Abrechnung erfolgt zu einem von Securepoint festgelegten Stichtag im Monat. Dieser ist in der Regel jeden Monat gleich.

Weiterentwicklung des Angebotes

Securepoint behält sich das Recht vor, einzeln angebotene Leistungen jederzeit zu erweitern, zu ergänzen oder zu verändern, sofern dies zu einer Verbesserung der Leistung für den Kunden führt bzw. keine oder keine wesentliche Beeinträchtigung dieser beinhaltet.

Allgemeines

Securepoint stellt die Plattform, einschließlich der hierüber zu erbringenden Leistungen, auf Servern zur Nutzung am Zugangspunkt des Rechenzentrums von Securepoint oder seiner Partner zur Verfügung („Übergabepunkt der Leistung“). Zur Nutzung der Plattform ist es erforderlich, dass der Kunde über einen eigenen Zugang zum Internet verfügt und über diesen Zugang auf die Plattform am Übergabepunkt der Leistung zugreift.

Der Kunde und seine Nutzer sind verpflichtet, die Login-Daten, Passwörter, etc. von den Accounts / User Accounts geheim zu halten und die Zugangsdaten nicht an unbefugte Dritte (oder andere Nutzer) weiterzugeben und sich nach jeder Anmeldung wieder abzumelden. Entsprechendes gilt bei einer Anmeldung via Single-Sign-On für die dort verwendeten Zugangsdaten, mit der Ausnahme, dass nicht nach jedem Zugang wieder eine manuelle Abmeldung erfolgen muss. Erklärungen und Handlungen, die nach einem Login über den Account / User Account mit dem Passwort und der E-Mail-Adresse des Kunden oder eines Nutzers abgegeben bzw. begangen werden, können dem Kunden auch dann zuzurechnen sein, wenn er hiervon keine Kenntnis hat. Eine Zurechnung erfolgt insbesondere dann, wenn der Kunde oder ein Nutzer Dritten (auch Familienangehörigen) vorsätzlich oder fahrlässig Zugang zum Passwort oder dem Account / User Account verschafft. Der Kunde hat den Anbieter im Falle eines begründeten Verdachts, dass Zugangsdaten unbefugten Dritten bekannt wurden, ist Securepoint aus Sicherheitsgründen berechtigt, aber nicht verpflichtet, nach freiem Ermessen die Zugangsdaten des Kunden oder des betreffenden Nutzers, ohne vorherige Ankündigung selbständig zu ändern bzw. die Nutzung des Accounts / User Accounts vorübergehend zu sperren. Securepoint informiert den Kunden bzw. Nutzer hierüber unverzüglich und teilt innerhalb angemessener Frist neue Zugangsdaten mit. Der Kunde bzw. Nutzer hat keinen Anspruch darauf, dass die ursprünglichen Zugangsdaten wiederhergestellt werden. Im Falle der Anmeldung via Single-Sign-On wird lediglich der Zugang via dieses Single-Sign-On mit den bisherigen Zugangsdaten gesperrt und der Kunde bzw. Nutzer kann sich nur noch über die neuen Zugangsdaten anmelden. Diese neuen Zugangsdaten können wiederum in einen Single-Sign-On integriert werden.

Die zeitgleiche Nutzung desselben Accounts über mehrere Endgeräte ist nicht erlaubt.

Sofern nicht ausdrücklich von Securepoint erlaubt, ist eine Registrierung der Nutzer mit privaten E-Mailadressen, insb. Freemailangeboten wie GMX, Web.de oder Google Mail nicht gestattet.

Nutzungs- und Urheberrechte

Securepoint räumt dem Kunden das örtlich unbeschränkte, befristete, widerrufliche, nicht-ausschließliche, nicht-unterlizenzierbare und nicht übertragbare Recht ein, die Plattform und die hierüber zur Verfügung gestellten Leistungsbausteine und Zusatzleistungen für die eigenen betrieblichen Zwecke für die in dem Vertrag über das Awareness-Building bestimmte Anzahl an Nutzern und vereinbarten Umfang zu nutzen.

Der Kunde ist nicht berechtigt, (i) die Plattform oder den Zugang zu der Plattform zu vermieten, zu verleasen, zu verleihen, zu reproduzieren, weiterzuverkaufen oder in sonstiger Weise zu vertreiben oder weiterzugeben, auch nicht über das Internet oder ein nachgelagertes öffentliches oder privates Datennetzwerk; (ii) die Plattform zur Entwicklung anderer Leistungen zu nutzen; (iii) Bestandteile der Plattform, für die dem Kunden keine Nutzungsrechte eingeräumt wurden, zu aktivieren oder zu nutzen; (iv) die Nutzungsrechte an der Plattform an Dritte zu übertragen oder Dritten Zugriff auf die Plattform zu gewähren; (v) den Programmcode der Plattform zu ändern, zu übersetzen, zu vervielfältigen, zu dekompileieren, seine Funktionen zu untersuchen, außer soweit gesetzlich zwingend gemäß § 69d oder § 69e UrhG zulässig; sowie (vi) rechtliche Hinweise, insbesondere auf gewerbliche Schutzrechte von Securepoint, zu entfernen, zu verdecken oder zu ändern.

Sofern Securepoint es dem Kunden ermöglicht, über die Plattform individuelle Materialien (Auswertungen des E-Learnings, Auswertungen der Phishing-Simulationen usw.) zu erstellen oder dem Kunden solche individuell für ihn erstellten Materialien zum Download oder Drucken zur Verfügung stellt, räumt Securepoint dem Kunden mit der vollständigen Zahlung der vereinbarten Vergütung die zeitlich und örtlich unbegrenzten, widerruflichen, nicht-ausschließlichen, nicht-unterlizenzierbaren und nicht-übertragbaren Nutzungsrechte an allen von Securepoint im Rahmen dieses Vertrages für den Kunden individuell erstellten Materialien ein, soweit die Übertragung nach deutschem Recht oder den tatsächlichen Verhältnissen möglich ist.

Die Nutzung der vorgenannten individuellen Materialien (ausgenommen aller fremden geschützten Marken oder Zeichen) und insbesondere der hierdurch gewonnenen Erkenntnisse zu eigenen Zwecken bleibt Securepoint vorbehalten.

Gewährleistung

Bezüglich der Nutzung der Plattform und der über die Plattform erbrachten Leistungsbausteine und Zusatzleistungen gelten bei Mängeln grundsätzlich die §§ 536 ff. BGB sowie die nachfolgenden Ziffern 3.2. bis 3.5.:

Die verschuldensunabhängige Haftung für anfängliche Mängel gemäß § 536a Abs. 1., 1. Var. BGB wird ausgeschlossen. Die verschuldensabhängige Haftung von Securepoint bleibt bestehen.

Die Behebung von Mängeln erfolgt nach Wahl von Securepoint entweder durch kostenfreie Nachbesserung oder Ersatzlieferung.

Eine Kündigung des Kunden gem. § 543 Abs. 2 S. 1 Nr. 1 BGB wegen Nichtgewährung des vertragsgemäßen Gebrauchs ist erst zulässig, wenn Securepoint ausreichende Gelegenheit zur Mängelbeseitigung gegeben wurde und diese fehlgeschlagen ist.

Securepoint übernimmt keine Gewährleistung für den Internet-Zugang des Kunden, insbesondere für die Verfügbarkeit und Dimensionierung des Internet-Zugangs. Der Kunde ist für seinen Internet-Zugang zum Übergabepunkt der Leistung selbst verantwortlich.

Service Level Agreement (SLA)

Geltungsbereich

Das Service Level Agreement konkretisiert und spezifiziert die Qualität sowie den Umfang der Leistungen, die die Securepoint GmbH (nachfolgend „Securepoint“) anbietet. Zwischen Securepoint und dem Kunden wird ein Vertrag zur Erbringung von Leistungen im Bereich MitarbeiterTraining / Awareness-Building geschlossen (im Folgenden „Hauptvertrag“). Der Leistungserbringer Securepoint und der Leistungsempfänger (nachfolgend „Kunde“) werden im Folgenden gemeinsam als „Parteien“ bezeichnet.

Dieses Dokument enthält alle relevanten Bestimmungen und Regelungen, durch welche die Leistungsbeschreibung der AwarenessBuilding-Leistungen und die Mitwirkungspflichten im Hauptvertrag zwischen den Parteien konkretisiert werden.

Voraussetzungen und Mitwirkungspflichten für die Nutzung der Leistungen

Allgemeine Voraussetzungen und Mitwirkungspflichten

Für diverse Bestandteile der nachfolgenden Leistungsbausteine (Ziffer 3) ist der Zugriff auf Webseiten von Securepoint mit einem Web-Browser erforderlich. Insoweit werden nur folgende Browser unterstützt und deren Verwendung bildet damit eine Voraussetzung für die Leistungserbringung: Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge und Microsoft Internet Explorer 11 in der jeweils aktuellen Version.

Spezielle Voraussetzungen und Mitwirkungspflichten

Die speziellen Voraussetzungen bzw. Mitwirkungspflichten für die Nutzung der Awareness-Building-Leistungen sind in Ziffer 3 bei den jeweiligen Leistungsbausteinen ausgeführt.

Leistungsbausteine

Die folgenden Abschnitte beschreiben die durch Securepoint angebotenen Leistungen und legen die Abläufe und organisatorischen Schnittstellen fest, die für eine Leistungserbringung erforderlich sind.

Phishing-Simulation

Der Leistungsbaustein Phishing-Simulation umfasst den Versand einer definierten Anzahl von (im Vorfeld abgestimmten) E-Mails an die Nutzer über den Leistungszeitraum. Diese E-Mails simulieren echte Phishing-Mails zur Steigerung der Awareness der Nutzer gegenüber IT-Sicherheitsrisiken durch Phishing-Angriffe. Beim Klick auf ein Phishing-Element (z. B. Bild, Link) in einer der simulierten Phishing-Mails wird eine Webseite aufgerufen (im Folgenden „Lernseite“), die den Nutzer über die Simulation aufklärt und konkrete Hinweise gibt, woran die jeweilige E-Mail als Phishing-Versuch hätte erkannt werden können.

Zur Sicherstellung der Zustellung aller simulierten Phishing-Mails an alle im Rahmen des Trainings zu schulenden Nutzer ist die Einrichtung eines Whitelisting durch den Kunden erforderlich. Es handelt sich hierbei um eine Mitwirkungspflicht des Kunden, ohne welche die Leistungserbringung durch Securepoint nicht gewährleistet werden kann. Der Kunde trägt somit an dieser Stelle die Verantwortung, dass die simulierten Phishing-Mails in vollständiger Form auch tatsächlich in den Postfächern der Nutzer ankommen und im Rahmen der Trainingsmaßnahme genutzt werden können. Kann der Kunde das Whitelisting selbst nicht beeinflussen (z. B. weil der Kunde einen IT-Dienstleister mit der Verwaltung seiner IT-Systeme beauftragt hat), so hat er dafür Sorge zu tragen, dass das Whitelisting dennoch erfolgt.

Für das Whitelisting müssen folgende Schritte unternommen werden:

Die dedizierten Mail-Server von Securepoint müssen im empfangenden Mail-System auf eine Whitelist gesetzt werden, um das Abweisen der eingehenden E-Mails zu verhindern.

Kundenseitig etwaig vorhandene Filtersysteme (z. B. Secure Mail-Gateway) sind entsprechend so zu konfigurieren, dass die simulierten Phishing-Mails nicht als „Junk“ oder „Spam“ markiert werden und die Zustellung an die Nutzer gewährleistet werden kann.

Kundenseitig etwaig vorhandene Systeme zum Zugriffsschutz auf das Internet von den Endgeräten der Nutzer aus (z. B. WebGateways, Proxys, Sicherheitseinstellungen des Betriebssystems) sind so zu konfigurieren, dass die unverfälschte Anzeige der simulierten Phishing-Mails in den E-Mail-Programmen der Nutzer gewährleistet ist. Des Weiteren sind diese Systeme so zu konfigurieren, dass die Lernseiten über einen Web-Browser anzeigbar sind.

Zur Umsetzung dieser Schritte wird durch Securepoint eine Anleitung bereitgestellt. Die Anleitung beinhaltet auch alle benötigten technischen Informationen wie IP-Adressen und Servernamen der Mail-Server, freizugebende URLs für Filtersysteme und Systeme zum Zugriffsschutz.

Zugriff über Lernplattform

Die proprietäre Lernplattform von Securepoint ist erreichbar unter <https://awareness.securepoint.cloud> - Hier können sich die Nutzer mit ihren beruflichen E-Mail-Adressen registrieren. Alternativ kann ein anonymer Zugangscode genutzt werden.

Securepoint Manager

Unter <https://manager.awareness.securepoint.cloud> ist der Securepoint Manager für den Kunden erreichbar. Der Securepoint Manager ist das Portal zur Administration der Awareness-Maßnahmen. Innerhalb des Reporting-Dashboards auf dem Portal kann der Kunde diverse Kennzahlen über die beauftragten Leistungsbestandteile einsehen, wie z. B. allgemeine Klickraten der simulierten Phishing-Mails, den Gesamtfortschritt im E-Learning oder -- je nach Leistungsvereinbarung -- auch individuelle E-Learning-Ergebnisse einzelner Mitarbeiter. Welche Daten genau einsehbar sind und verarbeitet werden, ist in einem separaten AV-Vertrag geregelt.

Leistungsumfang einzelner Awareness-Pakete

Das Paket ist für Kunden mit 1-250 Nutzern buchbar.

Dem Kunden wird auf der Self-Service-Plattform <https://wiki.securepoint.de> umfangreiche Anleitungen zur Verfügung gestellt, die alle notwendigen Schritte, wie z. B. die Einrichtung des Whitelistings, für einen Nutzer verständlich erklärt.

Über die Plattform müssen alle relevanten Informationen (Kundenstammdaten, Abrechnungsdaten etc.) kundenseitig eingetragen werden.

Für die Übermittlung der Nutzerliste wird eine Vorlage (Excel-Datei) zur Verfügung gestellt, deren Schema eingehalten werden muss, um einen sauberen Upload der Daten in die Self-Service-Plattform zu gewährleisten. Diese Nutzerliste kann kundenseitig aktualisiert werden.

Interaktive Lernmodule und Lernvideos im E-Learning sind fix und können nicht verändert werden. Für die Phishing-Simulation kann ein passendes Branchenpaket ausgewählt werden.

Für die Übermittlung der Nutzerliste für die Phishing-Simulation und/oder das E-Learning wird eine Vorlage (Excel-Datei) zur Verfügung gestellt, deren Schema eingehalten werden muss. Die

Übermittlung der Nutzerliste an Securepoint erfolgt über eine gesicherte Datenverbindung auf das Securepoint Manager Portal. Der Kunde erhält hierfür ein Nutzerkonto.

Eine Aktualisierung der Nutzerliste über den o.g. Zugang zum Securepoint Manager Portal kann der Kunde jederzeit selbstständig durchführen, sollten sich aufgrund von Fluktuation etc. Änderungen ergeben.

Für die Einrichtung des Whitelistings wird von Securepoint eine Anleitung zur Verfügung gestellt.

Für das E-Learning können aus den zur Verfügung stehenden interaktiven Lernmodulen und Lernvideos zum Thema IT-Sicherheit die vereinbarte Anzahl oder Auswahl für alle Nutzer des Kunden aktiviert werden.

Als Sprachen stehen Deutsch und Englisch zur Verfügung.

Für die Phishing-Simulation

Wir versenden randomisiert und über das Jahr verteilt 12 simulierte Phishing-Mails, die auf Angriffen basieren, die z.B. in Ihrer Branche beobachtet werden. Diese Sammlung wird laufend aktualisiert.

Als Sprachen stehen Deutsch und Englisch zur Verfügung.

Die Auswertung enthält Benchmarks zu allen Kennzahlen im Vergleich zum Kundendurchschnitt.

Bei Nutzung der Securepoint Lernplattform erhalten Nutzer ein Zertifikat über alle bestandenen Lernmodule.

Gamification: Auf der Securepoint Lernplattform durchlaufen Nutzer Levels, sammeln Abzeichen und können ihre Fortschritte in einer persönlichen Erfolgsübersicht einsehen. (An- und abschaltbar)

Verfügbarkeit der Dienste

Generelle Verfügbarkeit

Für Awareness-Building-Leistungen, die von Securepoint über <https://awareness.securepoint.cloud>, die Lernseiten oder den Streaming-Server erbracht werden, dürfen die nachfolgenden durchschnittlichen (bezogen auf das Monatsmittel) Verfügbarkeiten nicht unterschritten werden. Diese gelten als erfüllt, solange die tatsächliche Verfügbarkeit diesen Wert im Monatsmittel nicht unterschreitet.

Gemessen wird die Verfügbarkeit als Verhältnis von Uptime - also der Zeit, die der Service ordnungsgemäß bereit steht - zur Gesamtzeit, also Uptime plus Downtime (Ausfallzeit):

Verfügbarkeit = $\text{Uptime} / (\text{Uptime} + \text{Downtime})$

Verfügbarkeiten in Prozent - umgerechnet in Minuten für ein System, das 24 Stunden am Tag, an 365 Jahrestagen (24×365) zur Verfügung steht (8760 Stunden).

E-Learning-Plattform: 97 %

Streaming-Server von Securepoint (Zugriff via externe LMS): 97 %

Lernseiten zur Simulation: 97 %

Ausnahmen von der Verfügbarkeit

Nicht als Ausfallzeit im Sinne des vorgenannten, gelten Wartungsarbeiten an den Systemen von Securepoint und ihren Zulieferern, die für den Erhalt und die Sicherheit des laufenden Betriebes bzw. der Durchführung von Updates oder Upgrades notwendig sind.

In der Regel wird eine Wartung an Wochenenden zwischen Samstag 09:00 Uhr und Sonntag 18:00 Uhr oder nachts an jedem Wochentag in der Zeit zwischen 23:00 Uhr und 07:00 Uhr am nächsten Morgen durchgeführt. In Ausnahmefällen kann eine Systemwartung unter Berücksichtigung der geringstmöglichen Beeinträchtigung des laufenden Betriebs auch in allen übrigen Zeiten durchgeführt werden. In solchen Fällen informiert Securepoint den Kunden über geplante Systemwartungen so früh wie möglich, spätestens aber eine Kalenderwoche vor der Systemwartung.

Unterschreitung der Verfügbarkeit

Für jede Unterschreitung der monatlichen Generellen Verfügbarkeit um einen vollen Prozentpunkt, sofern nicht gemäß "Ausnahmen von der Verfügbarkeit" ausgeschlossen, erhält der Kunde einen zusätzlichen Tag der vereinbarten Leistungen am Ende der Vertragslaufzeit.