SaaS Security

Software as a Service

Managed Service: SaaS Security

Tractie houden op het beheren, configureren (inrichten), updaten, trainen voor en beleid van security oplossingen brengt veel tijd en kosten met zich mee voor een organisatie. Veel organisaties kampen met een beperkte IT security personeelscapaciteit en willen hier niet teveel mee belast worden. Met Amitron's Managed Service, behoudt uw organisatie de regie. Terwijl Amitron de adviserende en uitvoerende rol op zicht neemt. Support en controle rapportages zijn inbegrepen in onze Managed Services.

Inbegrepen in de Managed Service:

- Inrichting / installatie
- Configuratie
- Opstellen securitybeleid
- Periodieke health check
- Periodieke status rapportage
- Remote beheer
- Upgrade en updates
- Configuratie backup
- 24x7 servicedesk support

KPI's Service Level Agreement:

- First-Time Fix Percentage
- SLA gemiddelde reactietijd
- Openstaande kwesties / afgeronde kwesties
- Mean Time To Repair
- Beschikbaarheid systeem[1]

Managed Service contractvoorwaarden

- Minimale afname 1 jaar
- Op- en afschalen per vastgestelde periode
- Upfront facturatie voor contractduur

Toepassingsgebieden SaaS Security

Door toename en adoptie van SaaS applicaties (verSaaSing) wordt het risico van het lekken van gevoelige informatie en de noodzaak van de beveiliging hiervan groter. (Gevoelige) data kan via SaaS applicaties eenvoudig belanden op ongewenste, ongecontroleerde cloud omgevingen en op onbeheerde mobiele (privé) apparaten.

Door deze ontwikkelingen zijn SaaS Security oplossingen sterk in opkomst. Met dergelijke additionele security oplossingen komen er nieuwe eisen en vragen naar specifieke kennis omtrent de te configureren en te beheren security. Dit levert extra druk op de meestal al reeds drukke beheerafdelingen. Om security beheerafdelingen te ontlasten biedt Amitron deze additionele security oplossing alternatief aan als managed service SaaS Security.

Amitron ontzorgt organisaties hierin met de Managed Service: SaaS Security. De SaaS Security oplossing biedt inzicht, bescherming en controle op uw cloud omgeving, SaaS applicaties, en mobiele apparaten. Onderstaand vindt u de meest voorkomende toepassingsgebieden van SaaS Security.

[1] Exclusief geplande downtime.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

Toegangscontrole van (on-)beheerde apparaten

Toegangscontrole bepaalt specifiek wanneer, wie, waar, waarmee en hoe medewerkers toegang krijgen tot bedrijfsgegevens. Organisaties kunnen toegang tot het bedrijfsnetwerk blokkeren of (gelimiteerd) toestaan. Tevens kunnen organisaties specifieke toegangsniveaus toewijzen aan medewerkers op basis van hun gebruikersprofiel en toegangsrecht.

Voorbeeld | Een werknemer probeert in te loggen op de Office 365 omgeving. Op basis van het toegangsniveau vanaf een privé laptop, mobiele telefoon of geografische locatie kunnen organisaties het bekijken van OneDrive documenten toestaan, maar bijvoorbeeld het downloaden niet.

De SaaS Security oplossing:

- Kan onderscheid maken tussen beheerde en niet-beheerde (privé) apparaten (mobiel, laptop etc.). Met als resultaat dat de toegang tot het bedrijfsnetwerk vanuit apparaten naar wens, gedeeltelijk of volledig kan worden beperkt.

1.1 Shadow IT controle

Shadow IT omvat alle IT binnen organisaties die niet officieel is goedgekeurd. Het risico van shadow IT is dat werknemers gevoelige bedrijfsgegevens opslaan en verwerken in cloud applicaties die niet door de IT-afdeling worden beheerd of gecontroleerd.

Shadow IT vormt een grote bedreiging voor de beveiliging van bedrijfsinformatie. Dit controleverlies kan leiden tot datalekken, reputatieschade en financiële gevolgen (boetes).

De SaaS Security oplossing:

- Detecteert werknemers die toegang proberen te krijgen tot risicovolle niet-geautoriseerde cloud applicaties voor zakelijke doeleinden.
- Blokkeert een selectie of alle niet goedgekeurde cloud applicaties.
- Adviseert (optie) werknemers real-time middels een pop-up dat de cloud applicatie waar ze toegang tot proberen te krijgen, niet is toegestaan. Vervolgens wordt een toegestaan alternatief aangeboden (''coaching'') zonder een harde blokkade.
- Controleert of data geüpload wordt naar risicovolle niet-geautoriseerde cloud applicaties om datalekken te kunnen voorkomen.

1.2 Data Loss Prevention (DLP)

Gegevensverlies is een groot risico voor elke organisatie die naar een SaaS applicaties en publieke clouds migreert. SaaS applicaties zoals Office 365, G Suite en Dropbox zijn gebouwd om eenvoudig delen van informatie en samenwerken mogelijk te maken. Hoewel dit voor hogere productiviteit kan zorgen, vergroot dit ook de kans op datalekken. Het voorkomen van datalekken middels Data Loss Prevention is een aanwinst voor elke organisatie die gebruik maakt van verschillende SaaS applicaties. De Data Loss prevention in SaaS Security kan voortborduren op het DLP beleid welke al van toepassing is.

De SaaS Security oplossing:

- Detecteert en controleert gevoelige data in e-mail en SaaS applicaties
- Scant data in cloud applicaties en classificeert deze middels een API-connectie en via proxy-technologie.
- Past een watermerk en tagging toe voor tracking.
- Past Data Right Management toe op bestanden om extra authenticatie af te dwingen en meer.
- Integreert met bestaande DLP policies.
- Waarborgt consistent gegevensbescherming, zowel on-premise als in public cloud omgevingen.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

1.3 Identity en Access Management (IAM) & Single Sign On (SSO) op gebruikersniveau

De General Data Protection Regulation verplicht organisaties om hun werknemers zich te laten identificeren en verifiëren middels sterke 2 factor authenticatie, bij gebruik van cloud applicaties en devices die gevoelige persoonsgegevens bevatten. Dit kan dynamisch worden toegepast afhankelijk van het bepaalde risicoprofiel (wanneer, wie, waar, waarmee en hoe) van de gebruiker. Deze vorm van bescherming gaat veel verder dan het afdwingen van complexe wachtwoorden en wordt vaak ook toegepast voor gevoelige bedrijfsdata (intellectual property). Organisaties hebben inzicht nodig in de aanmeldingen van en controle over de gebruikers. Cloud identity, access management en SSO zijn een kerncomponent van de SaaS Security oplossing.

De SaaS Security oplossing:

- Past Multi Factor Authenticatie dynamisch toe op risicovolle situaties voor alle SaaS applicaties.
- Blokkeert of past gebruikerstoegang aan centraal aan met één actie.
- Biedt centrale gebruikerstoegang tot de SaaS applicaties.
- Registreert alle authenticatiepogingen voor auditing doeleinden.
- Biedt ingebouwde groeps- en gebruikersbeheer via Active Directory, single-sign-on en multi-factor authenticatie (MFA).
- Rolt gebruikers uit
- Integreert met de bestaande IAM, SSO oplossingen, maar kan ook zelfstandig worden ingezet.
- Integreert met een eventueel reeds actieve MFA oplossingen, maar kan ook zelfstandig worden ingezet.
- Heeft de noodzaak van speciale IDaaS-oplossingen overbodig gemaakt.

1.4 Secure Mobile Access

Traditioneel werd zakelijke mobiele apparatuur beveiligd en beheerd door het installeren van Mobile Device Management (MDM) security agents. Echter, door het toestaan van Bring-Your-Own-Device (BYOD), is bedrijfsdata tegenwoordig steeds vaker toegankelijk vanaf onbeheerde (privé) mobiele apparatuur. Via bijvoorbeeld het ActiveSync protocol. Organisaties verliezen hierdoor inzicht en controle over gevoelige data. Helaas is de installatie en managementcontrole van software agents op privé apparaten niet altijd een optie, met zicht op privacy inbreuk.

De SaaS Security oplossing:

- Gebruikt geen volledige managementcontrole op mobiele apparaten, maar trekt simpelweg de toegang tot zakelijke e-mail weg en delete deze van het bewuste apparaat. Er wordt dus niet ingegrepen op privacy inbreuk. Dit kan ook weer eenvoudig volledig hersteld worden. Bijvoorbeeld bij verlies en het terugvinden van het mobiele apparaat.
- Behoudt controle inzicht op (on)beheerde mobiele (privé) apparaten middels agentless mobiele gegevensbeschermingsmogelijkheden.
- Biedt additionele Mobile Device Management mogelijkheden, zoals het instellen van apparaat beveiligingsconfiguraties inclusief het gebruik opleggen van pincodes en dataversleuteling.
- Blokkeert, beperkt of staat toegang toe vanaf (on)beheerde privé apparaten naar bedrijfsdata:
  - Over het gebruik van de ActiveSync kan two-factor authenticatie toegepast worden.
  - Via DLP kan bedrijfsdata op gevoeligheid gecontroleerd worden.
  - Het bericht kan middels DLP geblokkeerd worden, of gevoelige data in het bericht aanpassen.
- Past selective wipe toe bij apparatuur verlies en diefstal. Selective wipe:
  - verwijdert alleen de bedrijfsgegevens van het onbeheerde apparaat
  - blokkeert toegang tot bedrijfsemail of SaaS applicaties, zonder schade toe te brengen aan de opgeslagen persoonlijke gegevens.
- Past eenvoudig een volledige restore toe van de mailbox.
- Kan worden geconfigureerd zonder het hoeven te installeren en beheren van software agents op onbeheerde (privé) apparaten.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

1.5 Analyse user behavior en cross-app visibility

Medewerkers kunnen bedrijfsbestanden opslaan in verschillende cloud applicaties die zijn ontwikkeld om eenvoudige samenwerking mogelijk maken. Dit complexe web van gebruikers, bestandstoegangen over meerdere applicaties en locaties vormt een beveiligingsuitdaging voor organisaties die bedrijfsgegevens controleren op legitieme gegevenstoegang of ongewenste toegang.

De SaaS Security oplossing:

- Biedt inzicht en controle op gegevenstoegang of ongewenst gedrag door een combinatie van gedetailleerde log- en gedragsanalyses van gebruikers (UEBA).
- Monitort werknemers en individuele bestanden middels logs audits, waardoor beheerders inzicht krijgen op uitgebreide, cross cloud applicaties.
- Onderneemt real time corrigerende acties en analyseert gebruikersacties real time.

Voorbeeld | Een gebruiker logt eerst in vanuit Europa in een Salesforce SaaS applicatie en binnen 5 minuten probeert dezelfde gebruiker in te loggen in Office 365 vanuit een ander continent of land. SaaS Security kan deze abnormale afwijking detecteren en direct actie ondernemen door deze gebruiker bijvoorbeeld een additionele authenticatie stap uit te laten voeren met een multi-factor authenticatie (MFA), voordat deze gebruiker toegang krijgt tot Office 365.

1.6 Controle op externe cloud datasharing

Een van de grootste voordelen van de cloud is het eenvoudig en snel data te kunnen delen en samenwerken. Dit voordeel brengt echter het risico van on- en bedoelde datalekken met zich mee.

Of een medewerker nu onzorgvuldig is of dat er kwaadaardige opzet in het spel is, gevoelige data kan heel snel en eenvoudig gedeeld worden met personen buiten de organisatie.

De SaaS Security oplossing:

- Levert controle op cloud sharing applicaties.
- Scant applicaties zoals Office 365 (OneDrive, SharePoint) en Google Drive op ongewenste externe data-shares en trekt deze eventueel in.
- Kan toegangscontrole fijnmazig geconfigureren om toegang tot privé e-mailadressen, vanaf onbeheerde apparaten of werknemers die zich niet op locatie bevinden etc., te weigeren.
- Volgt bestanden op het moment deze worden gedownload door onbevoegden middels een DLP beleid zoals watermerken en tagging.

1.7 Stop cloud malware en ransomware in SaaS

Malware uitbraken zoals WannaCry ransomware in 2017, is een duidelijk voorbeeld van waarom organisaties geavanceerde antimalware- en ransomware bescherming nodig hebben. Vanwege het gebruik van decentrale cloudapplicaties en Bring Your Own Devices (BYOD) hebben bedreigingen tegenwoordig meer toegangspunten om op toe te slaan. Door het uploaden of syncen van één enkel besmet bestand naar een cloud applicatie, kan malware zich razendsnel verspreiden binnen en buiten de organisatie (indien er connectie met deze cloud wordt gemaakt).

Helaas is bij het merendeel van de cloud applicaties geen adequate, centrale, ransomware-bescherming ingebouwd. Hierdoor wordt de noodzakelijke bescherming voor deze cloud applicaties een verantwoordelijkheid van de organisatie zelf.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

De SaaS Security oplossing:

- Biedt centrale, geïntegreerde, geavanceerde antimalware- en ransomware bescherming tegen dergelijke zero-day malware dreigingen (ATP), middels de nieuwste sandbox technieken.
- Beschermt in-line tussen de gebruiker en de cloud applicatie in, waardoor alle zero-day bedreigingen worden ondervangen.
- Scant data in cloud applicaties middels een API-connectie en via proxy op reeds aanwezige malware en nog niet actieve ransomware.
- Voorkomt dat deze reeds aanwezige malware en nog niet actieve ransomware onbewust worden gesynct, gedownload of verspreid naar andere apparaten of geconnecteerde cloud applicaties.

1.8 Dataversleuteling at rest

Sommige organisaties zijn verplicht door strenge wettelijke regelgeving of compliance regels, data te versleutelen indien dit op publieke omgevingen wordt geplaatst (zogenoemde data-at-rest). Voor cloud applicatie (SaaS) aanbieders, die hun eigen dataversleuteling beschikbaar stellen binnen de SaaS dienst, is het altijd technisch mogelijk om data te bekijken. Dit komt omdat de cloud applicatie aanbieders de privé sleutel in handen hebben van hun SaaS dienst, waarmee data ontsleuteld kan worden.

Het versleutelen van deze data-at-rest is geen makkelijke taak. Het toepassen van additionele derde partij versleuteloplossingen (encryptie) verbreekt vaak belangrijke toepassingsfuncties uit de SaaS dienst zoals data sorteren en zoeken. Of verzwakt versleuteling om bepaalde functionaliteiten in de SaaS dienst mogelijk te maken.

De SaaS Security oplossing:

- Past standaard versleuteling toe op de dataconnectie over het internet, voor de data-in-motion.
- Versleutelt en beschermt bedrijfsdata in de cloud tegen ongeautoriseerde gebruikers.
- Beschermt bedrijfsdata tegen (mogelijk ongewenst) inzicht van cloud applicatie aanbieders door het gebruik van eigen encryptiesleutels.
- Voorkomt verlies van belangrijke SaaS dienst functionaliteit door zogenaamde veldniveau gegevens in SaaS diensten, zoals Salesforce, op dezelfde manier te versleutelen.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl