SAML (!)

Was ist SAML?

SAML steht für **S**ecurity **A**ssertion **M**arkup **L**anguage. Die Hauptrolle von SAML bei der Online-Sicherheit besteht darin, den Zugriff auf mehrere Webanwendungen mit einem einzigen Satz von Anmeldeinformationen zu ermöglichen. Auf Basis des XML-Formats (Extensible Markup Language) werden Authentifizierungsinformationen in einem bestimmten Format zwischen zwei Parteien, in der Regel einem Identitätsanbieter (Identity Provider, idp) und einer Webanwendung, übermittelt

Warum wurde SAML entwickelt?

SAML wurde entwickelt, um den Authentifizierungsprozess zu vereinfachen, wenn Benutzer auf mehrere voneinander unabhängige Webanwendungen in verschiedenen Domänen zugreifen müssen. Der Hauptzweck liegt bei der Zentralisierung der Benutzerauthentifizierung bei einem Identitätsanbieter. Webanwendungen können SAML über den Indentitätsanbieter nutzen, um ihren Benutzern Zugriff zu gewähren. Durch diesen SAML-Authentifizierungsansatz müssen sich Benutzer nicht mehrere Benutzernamen und Kennwörter merken. Auch die Serviceanbieter profitieren davon, da sie die Sicherheit ihrer eigenen Plattform erhöhen, vor allem, weil sie keine (oft schwachen und unsicheren) Kennwörter speichern und sich nicht um vergessene Kennwörter kümmern müssen.

Wie funktioniert SAML?

SAML funktioniert durch den Austausch von Benutzerinformationen wie Anmeldung, Authentifizierungsstatus, Kennungen und anderen relevanten Attributen zwischen dem Identitätsanbieter und dem Serviceanbieter. Dadurch wird der Authentifizierungsprozess einfacher und sicherer, da sich der Benutzer nur einmal mit einem einzigen Satz von Anmeldeinformationen zur Authentifizierung anmelden muss. Wenn der Benutzer also versucht, auf eine Website zuzugreifen, gibt der Identitätsanbieter die SAML-Authentifizierung an den Serviceanbieter weiter, der dem Benutzer dann Zugriff gewährt.

Unternehmen müssen oft die Identität des Benutzers bestätigen, bevor Sie Zugriff gewähren können. Ein gutes Beispiel dafür ist die Luftfahrtbranche. Bevor man ein Flugzeug besteigen kann, muss die Fluggesellschaft bestätigen, dass man derjenige ist, für den man sich ausgibt, um die Sicherheit der anderen Fluggäste zu gewährleisten. Daher wird die Identität anhand eines amtlichen Lichtbildausweises überprüft. Sobald bestätigt ist, dass der Name auf dem Ausweis mit dem Namen auf dem Flugticket übereinstimmt, darf man das Flugzeug betreten.

In diesem Beispiel ist der Staat der Identitätsanbieter und die Fluggesellschaft der Serviceanbieter. Der amtliche Ausweis ist die SAML-Assertion (XML-Dokument, das der Identitätsprovider an den Dienstanbieter sendet). Wenn man einen Personalausweis beantragt, muss man in der Regel ein Formular ausfüllen, ein Foto machen lassen und unter Umständen auch einen Fingerabdruck abgeben. Der Staat (Identitätsanbieter) speichert dann diese identifizierenden Attribute in seiner Datenbank und stellt einem einen physischen Ausweis aus, der mit der eigenen Identität verbunden ist. Im Flug-Beispiel prüft die Fluggesellschaft (der Serviceanbieter) bei der Ankunft am Gate die Identitätsbestätigung (SAML). Die Fluggesellschaft akzeptiert den Personalausweis, da er die eigenen Angaben enthält und als gültiges Dokument erachtet wird. Nach erfolgreicher Authentifizierung erlaubt die Fluggesellschaft einem das Flugzeug zu betreten.

blocked URL

Anwendungsbeispiel

1. Der Benutzer öffnet seinen Browser und navigiert zur Webanwendung des Serviceanbieter (Anwendung von Chrome, Office365, o.ä), die einen Identitätsanbieter(Mircosoft Active Directory, Azure, o.ä) für die Authentifizierung verwendet
2. Die Webanwendung antwortet mit einer SAML-Anfrage
3. Der Browser leitet die SAML-Anfrage an den Identitätsanbieter weiter
4. Der Identitätsanbieter analysiert die SAML-Anfrage
5. Der Identitätsanbieter authentifiziert den Benutzer, indem er ihn zur Eingabe eines Benutzernamens und eines Kennworts oder eines anderen Authentifizierungsfaktors auffordert. Der Identitätsanbieter überspringt diesen Schritt, wenn der Benutzer bereits authentifiziert ist
6. Der Identitätsanbieter generiert die SAML-Antwort und sendet sie an den Browser des Benutzers zurück
7. Der Browser sendet die generierte SAML-Antwort an die Webanwendung des Serviceanbieters die sie verifiziert.
8. Wenn die Überprüfung erfolgreich ist, gewährt die Webanwendung dem Benutzer Zugriff.