# nevisAuth – End-to-End-Verschlüsselung

## Vorteile

End-to-End-Verschlüsselung: WhatsApp und Viber haben es, Facebook macht es und bald wird auch Google so weit sein. Und auch NEVIS unterstützt diese Funktion und verschlüsselt Login-Daten der Benutzer auf ihrem Weg vom Benutzergerät zum Server. So kann kein Dritter geheime Zugangsdaten lesen, die zwischen den an der Kommunikation beteiligten Parteien ausgetauscht werden. Somit

- **kann niemand mehr vertraulichen Datenverkehr abhören** und
- **die Sicherheit Ihres Systems wird verbessert**, da
- **es besser gegen Angriffe und Identitätsdiebstahl geschützt ist.**

## Worum geht es?

Bei mit End-to-End-Verschlüsselung geschützter Kommunikation können nur die Beteiligten die Nachrichten lesen. Das Mitlesen der Kommunikation während der Übertragung, böswillig oder nicht, ist unmöglich. Die Inhalte werden mit einem speziellen kryptografischen Algorithmus verschlüsselt. Nur der Absender und der Empfänger der Daten besitzen die zur Entschlüsselung notwendigen Schlüssel.

Die End-to-End-Verschlüsselung in NEVIS ist als „Formularverschlüsselung“ ausgeführt. Sie unterstützt die Verschlüsselung von Benutzername, Passwort und allen anderen Daten, die der Benutzer in ein Login-Formular eingibt. Dies schützt die Benutzer-Zugangsdaten auf ihrem Weg vom Benutzer zum Authentisierungsserver im Backend. Ausserdem sind Klartext-Passwörter davor geschützt, während der Übertragung zwischen Client und Server unbeabsichtigt in eine Protokolldatei aufgenommen zu werden.

Ihre vertraulichen Informationen sind also gegen Angriffe Dritter gesichert, insbesondere gegen passive Angriffe, bei denen Ihr System einfach abgehört und überwacht wird, um Informationen zu erhalten. Mit End-to-End-Verschlüsselung ist es nun unmöglich, ihre geheimen Daten abzuhören. Nicht einmal nevisProxy kann verschlüsselte Benutzerpasswörter entschlüsseln!

Und dies hat seinen Grund. Nehmen wir an, ein Benutzer möchte in einer typischen NEVIS-Umgebung ohne Formularverschlüsselung auf eine Unternehmensanwendung zugreifen. Zunächst stellt der Client-PC oder das mobile Gerät des Benutzers eine Verbindung mit nevisProxy her. Der Proxyserver befindet sich zwischen dem Client-Gerät und der Unternehmensanwendung. Er kontrolliert die Zugangsdaten des Benutzers und schützt Ihr System gegen interne und externe Bedrohungen.

Während des Login-Vorgangs sendet der Benutzer seine Zugangsdaten über eine sichere Verbindung an den Proxyserver. Der Proxyserver leitet seinerseits den Benutzernamen und das Passwort an nevisAuth weiter, das für die Benutzerauthentisierung zuständig ist. Sind die Login-Daten des Benutzers nicht verschlüsselt, kann der Proxy den Benutzernamen und das Passwort während des Sendens der Daten an nevisAuth lesen. Es wäre sogar möglich, dass die Zugangsdaten im Klartext und unverschlüsselt in einer Protokolldatei abgelegt werden.

Dass dies ein Sicherheitsrisiko ist, versteht sich von selbst. Um die vertraulichen Benutzerdaten besser zu schützen, führt NEVIS die Verschlüsselung der Benutzerdaten mittels eines Login-Formulars ein. Die Verschlüsselungsfunktion ist in die HTML-basierte Login-Seite integriert. Sie wird aktiviert, sobald der Benutzer die Seite aufruft.



Schweiz ▪ AdNovum Informatik AG ▪ Röntgenstrasse 22 ▪ 8005 Zürich ▪ Schweiz ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapur ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Deutschland ▪ NEVIS Security GmbH ▪ Maximilianstraße 35 A ▪ 80539 München ▪ Deutschland ▪ +49 89 2421 8180 ▪ info@nevis-security.de ▪ www.nevis-security.de

## Wichtigste Merkmale

- Verhindert, dass das System Benutzer-Zugangsdaten unverschlüsselt in einer Protokolldatei ablegt.
- Schützt gegen passive sicherheitsrelevante Angriffe, beispielsweise gegen Abhören.
- Verschlüsselt alle Benutzer-Zugangsdaten unabhängig, um die Sicherheit zu erhöhen.
- Führt die Verschlüsselung automatisch im Hintergrund aus, ohne jegliche Beeinträchtigung des Nutzererlebnisses oder des einfachen Zugangs.
- Ermöglicht flexible Länge/Stärke der Schlüssel, um sämtlichen Sicherheitsanforderungen gerecht zu werden.
- Gestattet gleichzeitig symmetrische und asymmetrische Verschlüsselung und vereint daher die Vorteile beider Verschlüsselungstechniken. (Bei symmetrischer Verschlüsselung wird für das Ver- und Entschlüsseln der gleiche Schlüssel verwendet. Asymmetrische Verschlüsselungsverfahren verwenden unterschiedliche Schlüssel für das Ver- und Entschlüsseln.)
- Unterstützt derzeit den AES-Verschlüsselungsalgorithmus in Verbindung mit öffentlichen und privaten RSA-Schlüsseln.

## Architektur

Abbildung 1 vergleicht den Schutz von Benutzer-Zugangsdaten mit und ohne Verschlüsselung. In beiden Fällen werden die Benutzer-Login-Daten mittels sicherem HTTPS-Protokoll (Hypertext Transfer Protocol Secure) und TLS-Protokoll (Transport Layer Security) vom Client zum nevisProxy-Server übertragen. Die Kommunikation findet also in einem sicheren Tunnel statt (Nr. 1 in der Abbildung).

Sobald sich die Zugangsdaten aber im Proxy befinden, gibt es keinen sicheren Tunnel mehr.

Ohne Verschlüsselung sind Benutzername und Passwort relativ ungeschützt und können Angriffen ausgesetzt sein (2). Werden die Benutzer-Zugangsdaten jedoch verschlüsselt, sind sie während der gesamten Übertragung vom Client-Gerät zum Authentisierungsserver geschützt (3). Erst bei der Authentisierung selbst werden die Zugangsdaten entschlüsselt und damit lesbar (4).

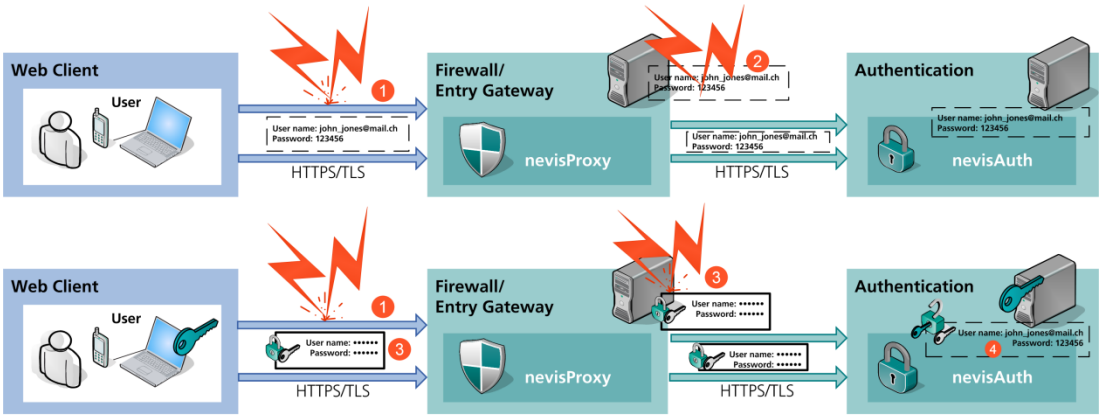


**Abbildung 1** Architekturüberblick



Schweiz ▪ AdNovum Informatik AG ▪ Röntgenstrasse 22 ▪ 8005 Zürich ▪ Schweiz ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapur ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Deutschland ▪ NEVIS Security GmbH ▪ Maximilianstraße 35 A ▪ 80539 München ▪ Deutschland ▪ +49 89 2421 8180 ▪ info@nevis-security.de ▪ www.nevis-security.de