

Cả 2 thuật ngữ thường được sử dụng kết hợp với nhau để nói về bảo mật, đặc biệt là khi nói đến quyền truy cập vào hệ thống. Cả hai đều là những chủ đề rất quan trọng thường đi kèm với các trang web như phần quan trọng trong cơ sở hạ tầng dịch vụ của mình. Tuy nhiên, cả hai thuật ngữ rất khác nhau với các khái niệm hoàn toàn khác nhau. Trong khi đó chúng thường được sử dụng trong bối cảnh tương tự với công cụ tương tự, chúng là hoàn toàn khác biệt với nhau.

Authentication (xác thực) có nghĩa là xác nhận danh tính của riêng bạn, trong khi authorization (ủy quyền) có nghĩa là cấp quyền truy cập vào hệ thống. Nói một cách đơn giản, authentication là quá trình xác minh bạn là ai, trong khi authorization là quá trình xác minh những gì bạn có quyền truy cập.

Authentication

Authentication là về việc xác thực thông tin đăng nhật của bạn như Username/User ID và mật khẩu. Trong các mạng network public hoặc private, hệ thống xác thực danh tính người dùng thông qua mật khẩu đăng nhập. Authentication thường được thực hiện bởi tên người dùng và mật khẩu, và đôi khi kết hợp với yếu tố xác thực, trong đó đề cập đến các cách khác nhau để được xác thực.

Các Authentication factor xác định các yếu tố khác nhau mà hệ thống sử dụng để xác minh một danh tính trước khi cấp cho anh ta quyền truy cập vào bất cứ điều gì từ việc truy cập file đến yêu cầu giao dịch ngân hàng. Một danh tính người dùng có thể được xác định bởi những gì anh ta biết, những gì anh ta có. Khi nói đến bảo mật, ít nhất hai hoặc cả ba yếu tố xác thực phải được xác minh để cấp cho ai đó quyền truy cập vào hệ thống.

Dựa trên cấp độ bảo mật, authentication factor có thể thay đổi theo một trong các cách sau:

* **Single-Factor Authentication** - Nó là phương thức xác thực đơn giản nhất thường dựa vào mật khẩu đơn giản để cấp cho người dùng quyền truy cập vào một hệ thống cụ thể là một website hoặc network. Người này có thể yêu cầu quyền truy cập vào hệ thống chỉ bằng một trong các thông tin đăng nhập để xác minh danh tính của mình. Ví dụ phổ biến nhất về xác thực một yếu tố sẽ là thông tin đăng nhập chỉ yêu cầu mật khẩu đối với tên người dùng hoặc địa chỉ email.
* **Two-Factor Authentication** - Như tên của nó, nó có một quy trình xác minh gồm hai bước, không chỉ yêu cầu tên người dùng và mật khẩu, mà còn một thứ mà chỉ người dùng biết, để đảm bảo mức độ bảo mật bổ sung, chẳng hạn như pin ATM, chỉ người dùng mới biết. Sử dụng tên người dùng và mật khẩu cùng với một thông tin bí mật bổ sung khiến cho những kẻ lừa đảo hầu như không thể đánh cắp dữ liệu có giá trị.
* **Multi-Factor Authentication** - Nó có một phương thức xác thực tiên tiến nhất sử dụng hai hoặc nhiều mức bảo mật từ các loại xác thực độc lập để cấp quyền truy cập cho người dùng vào hệ thống. Tất cả các yếu tố phải độc lập với nhau để loại bỏ bất kỳ lỗ hổng nào trong hệ thống. Các tổ chức tài chính, ngân hàng và các cơ quan thực thi pháp luật sử dụng xác thực nhiều yếu tố để bảo vệ dữ liệu và ứng dụng của họ khỏi các mối đe dọa tiềm ẩn.

Ví dụ: khi bạn nhập thẻ ATM vào máy ATM, máy sẽ yêu cầu bạn nhập mã pin. Sau khi bạn nhập mã pin chính xác, ngân hàng sẽ xác nhận danh tính của bạn rằng thẻ thực sự thuộc về bạn và bạn là chủ sở hữu hợp pháp của thẻ. Bằng cách xác nhận mã pin thẻ ATM của bạn, ngân hàng thực sự xác minh được danh tính của bạn, được gọi là authentication. Nó chỉ đơn thuần xác định bạn là ai, không có gì khác.

**Authorization**

Mặt khác, Authorization xảy ra sau khi hệ thống của bạn được authentication (xác thực) thành công, cuối cùng cho phép bạn toàn quyền truy cập các tài nguyên như thông tin, file, cơ sở dữ liệu, quỹ, địa điểm, hầu hết mọi thứ. Nói một cách đơn giản, authorization xác định khả năng của bạn để truy cập hệ thống và ở mức độ nào. Khi danh tính của bạn được hệ thống xác minh sau khi xác thực thành công, bạn sẽ được phép truy cập tài nguyên của hệ thống.

Authorization là quá trình để xác định xem người dùng được xác thực có quyền truy cập vào các tài nguyên cụ thể hay không. Nó xác minh quyền của bạn để cấp cho bạn quyền truy cập vào các tài nguyên như thông tin, cơ sở dữ liệu, file, v.v. Authorization thường được đưa ra sau khi xác thực xác nhận các đặc quyền của bạn để thực hiện. Nói một cách đơn giản hơn, nó giống như cho phép ai đó chính thức làm điều gì đó hoặc bất cứ điều gì.

Ví dụ, quy trình xác minh và xác nhận ID nhân viên và mật khẩu trong một tổ chức được gọi là authentication, nhưng xác định nhân viên nào có quyền truy cập vào tầng nào được gọi là authorization. Hãy nói với bạn rằng bạn đang đi du lịch và bạn sẽ lên một chuyến bay. Khi bạn xuất trình vé và một số giấy tờ tùy thân trước khi nhận phòng, bạn sẽ nhận được thẻ lên máy bay xác nhận rằng cơ quan sân bay đã xác thực danh tính của bạn. Nhưng đó không phải là nó. Một tiếp viên hàng không phải ủy quyền cho bạn lên chuyến bay mà bạn được cho là đang bay, cho phép bạn truy cập vào bên trong máy bay và các tài nguyên của nó.

Truy cập vào một hệ thống được bảo vệ bởi cả authentication và authorization. Mọi nỗ lực truy cập hệ thống có thể được xác thực bằng cách nhập thông tin xác thực, nhưng chỉ có thể được chấp nhận sau khi ủy quyền thành công. Nếu nỗ lực được xác thực nhưng không được phép, hệ thống sẽ từ chối quyền truy cập vào hệ thống.

| **Authentication** | **Authorization** |
| --- | --- |
| Authentication xác nhận danh tính của bạn để cấp quyền truy cập vào hệ thống. | Authorization xác định xem bạn có được phép truy cập tài nguyên không. |
| Đây là quá trình xác nhận thông tin đăng nhập để có quyền truy cập của người dùng. | Đó là quá trình xác minh xem có cho phép truy cập hay không. |
| Nó quyết định liệu người dùng có phải là những gì anh ta tuyên bố hay không. | Nó xác định những gì người dùng có thể và không thể truy cập. |
| Authentication thường yêu cầu tên người dùng và mật khẩu. | Các yếu tố xác thực cần thiết để authorization có thể khác nhau, tùy thuộc vào mức độ bảo mật. |
| Authentication là bước đầu tiên của authorization vì vậy luôn luôn đến trước. | Authorization được thực hiện sau khi authentication thành công. |
| Ví dụ, sinh viên của một trường đại học cụ thể được yêu cầu tự xác thực trước khi truy cập vào liên kết sinh viên của trang web chính thức của trường đại học. Điều này được gọi là authentication. | Ví dụ, authorization xác định chính xác thông tin nào sinh viên được phép truy cập trên trang web của trường đại học sau khi authentication thành công. |

Tài liệu: <http://www.differencebetween.net/technology/difference-between-authentication-and-authorization/>