FEATURE

What is access control? A key component of data security

Access controls authenticate and authorize individuals to access the information they are allowed to see and use.

By James A. Martin

CSO | AUG 21, 2019 3:00 AM PDT

ages

Who should access your company's data? How do you make sure those who attempt access have actually been granted that access? Under which circumstances do you deny access to a user with access privileges?

To effectively protect your data, your organization's access control policy must address these (and other) questions. What follows is a guide to the basics of access control: What it is, why it's important, which organizations need it the most, and the challenges security professionals can face.

What is access control?

Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data.

At a high level, access control is a selective restriction of access to data. It consists of two main components: authentication and authorization, says Daniel Crowley, head of research for IBM’s X-Force Red, which focuses on data security.

Authentication is a technique used to verify that someone is who they claim to be. Authentication isn’t sufficient by itself to protect data, Crowley notes. What’s needed is an additional layer, authorization, which determines whether a user should be allowed to access the data or make the transaction they’re attempting.

Without authentication and authorization, there is no data security, Crowley says. “In every data breach, access controls are among the first policies investigated,” notes Ted Wagner, CISO at SAP National Security Services, Inc. “Whether it be the inadvertent exposure of sensitive data improperly secured by an end user or the Equifax breach, where sensitive data was exposed through a public-facing web server operating with a software vulnerability, access controls are a key component. When not properly implemented or maintained, the result can be catastrophic.”

Any organization whose employees connect to the internet—in other words, every organization today—needs some level of access control in place. “That’s especially true of businesses with employees who work out of the office and require access to the company data resources and services,” says Avi Chesla, CEO of cybersecurity firm empow.

Put another way: If your data could be of any value to someone without proper authorization to access it, then your organization needs strong access control, Crowley says.

Another reason for strong access control: Access mining

The collection and selling of access descriptors on the dark web is a growing problem. For example, a new report from Carbon Black describes how one cryptomining botnet, Smominru, mined not only cryptcurrency, but also sensitive information including internal IP addresses, domain information, usernames and passwords. The Carbon Black researchers believe it is "highly plausible" that this threat actor sold this information on an "access marketplace" to others who could then launch their own attacks by remote access.

These access marketplaces "provide a quick and easy way for cybercriminals to purchase access to systems and organizations.... These systems can be used as zombies in large-scale attacks or as an entry point to a targeted attack," said the report's authors. One access marketplace, Ultimate Anonymity Services (UAS) offers 35,000 credentials with an average selling price of $6.75 per credential.

The Carbon Black researchers believe cybercriminals will increase their use of access marketplaces and access mining because they can be "highly lucrative" for them. The risk to an organization goes up if its compromised user credentials have higher privileges than needed.

Access control policy: Key considerations

Most security professionals understand how critical access control is to their organization. But not everyone agrees on how access control should be enforced, says Chesla. “Access control requires the enforcement of persistent policies in a dynamic world without traditional borders,” Chesla explains. Most of us work in hybrid environments where data moves from on-premises servers or the cloud to offices, homes, hotels, cars and coffee shops with open wi-fi hot spots, which can make enforcing access control difficult.

“Adding to the risk is that access is available to an increasingly large range of devices,” Chesla says, including PCs, laptops, smart phones, tablets, smart speakers and other internet of things (IoT) devices. “That diversity makes it a real challenge to create and secure persistency in access policies.”

In the past, access control methodologies were often static. “Today, network access must be dynamic and fluid, supporting identity and application-based use cases,” Chesla says.

A sophisticated access control policy can be adapted dynamically to respond to evolving risk factors, enabling a company that's been breached to “isolate the relevant employees and data resources to minimize the damage,” he says.

Enterprises must assure that their access control technologies “are supported consistently through their cloud assets and applications, and that they can be smoothly migrated into virtual environments such as private clouds,” Chesla advises. “Access control rules must change based on risk factor, which means that organizations must deploy security analytics layers using AI and machine learning that sit on top of the existing network and security configuration. They also need to identify threats in real-time and automate the access control rules accordingly.”

4 Types of access control

Organizations must determine the appropriate **access control model** to adopt based on the type and sensitivity of data they're processing, says Wagner. Older access models include discretionary access control (DAC) and mandatory access control (MAC), role based access control (RBAC) is the most common model today, and the most recent model is known as attribute based access control (ABAC).

Discretionary access control (DAC)

With DAC models, the data owner decides on access. DAC is a means of assigning access rights based on rules that users specify.

Mandatory access control (MAC)

MAC was developed using a nondiscretionary model, in which people are granted access based on an information clearance. MAC is a policy in which access rights are assigned based on regulations from a central authority.

Role Based Access Control (RBAC)

RBAC grants access based on a user's role and implements key security principles, such as “least privilege” and “separation of privilege.” Thus, someone attempting to access information can only access data that’s deemed necessary for their role.

Attribute Based Access Control (ABAC)

In ABAC, each resource and user are assigned a series of attributes, Wagner explains. “In this dynamic method, a comparative assessment of the user’s attributes, including time of day, position and location, are used to make a decision on access to a resource.”

It’s imperative for organizations to decide which model is most appropriate for them based on data sensitivity and operational requirements for data access. In particular, organizations that process personally identifiable information (PII) or other sensitive information types, including Health Insurance Portability and Accountability Act (HIPAA) or Controlled Unclassified Information (CUI) data, must make access control a core capability in their security architecture, Wagner advises.

Access control solutions

A number of technologies can support the various access control models. In some cases, multiple technologies may need to work in concert to achieve the desired level of access control, Wagner says.

“The reality of data spread across cloud service providers and SaaS applications and connected to the traditional network perimeter dictate the need to orchestrate a secure solution,” he notes. “There are multiple vendors providing privilege access and identity management solutions that can be integrated into a traditional Active Directory construct from Microsoft. Multifactor authentication can be a component to further enhance security.”

Why authorization remains a challenge

Today, most organizations have become adept at authentication, says Crowley, especially with the growing use of multifactor authentication and biometric-based authentication (such as facial or iris recognition). In recent years, as high-profile data breaches have resulted in the selling of stolen password credentials on the dark web, security professionals have taken the need for multi-factor authentication more seriously, he adds.

Authorization is still an area in which security professionals "mess up more often," Crowley says. It can be challenging to determine and perpetually monitor who gets access to which data resources, how they should be able to access them, and under which conditions they are granted access, for starters. But inconsistent or weak authorization protocols can create security holes that need to be identified and plugged as quickly as possible.

Speaking of monitoring: However your organization chooses to implement access control, it must be constantly monitored, says Chesla, both in terms of compliance to your corporate security policy as well as operationally, to identify any potential security holes. "You should periodically perform a governance, risk and compliance review," he says. "You need recurring vulnerability scans against any application running your access control functions, and you should collect and monitor logs on each access for violations of the policy."

In today's complex IT environments, access control must be regarded as "a living technology infrastructure that uses the most sophisticated tools, reflects changes in the work environment such as increased mobility, recognizes the changes in the devices we use and their inherent risks, and takes into account the growing movement toward the cloud," Chesla says.

More on access control:

- **5 steps to simple role-based access control (RBAC)**
- **Role-based access control is fine – who needs attribute-based access control?**
- **HP gives software robots their own IDs to audit their activities**
- **What is identity management? IAM definition, uses, and solutions**
- **The best identity management advice right now**
- **What is SAML? How it works and how it enables single sign on**
- **What is OAuth? How the open authorization framework works**

Next read this

- *The new CISO's playbook: 5 rules to follow*
- *7 hot cybersecurity trends (and 4 going cold)*
- *Top cyber security certifications: Who they're for, what they cost, and which you need*
- *The best password advice right now (Hint: It's not the NIST guidelines)*
- *8 cheap or free cybersecurity training resources*
- *24 best free security tools*
- *8 cheap or free cybersecurity training resources*
- *Top cyber security certifications: Who they're for, what they cost, and which you need*
- *12 tips for effectively presenting cybersecurity to the board*

Related: Access Control Authentication Data Security Security Identity Management

James A. Martin is a seasoned tech journalist and blogger based in San Francisco and winner of the 2014 ASBPE National Gold award for his Living the Tech Life blog on CIO.com. James is also a content marketing consultant.

Follow

Cryptojacking worm infects exposed Docker

Homepage

Rising complexity, higher stakes for enterprise risk

Homepage

Top Linux antivirus software

Homepage

ABOUT US | CONTACT | PRIVACY POLICY | COOKIE POLICY | MEMBER PREFERENCES | ADVERTISING | IDG CAREERS | AD CHOICES | E-COMMERCE LINKS

Explore the IDG Network ▼