How context-aware security adds layers of protection to single sign-on services

By François Amigorena, CEO, IS Decisions

Single sign-on, to the user, is a godsend. No more wasting time putting in passwords to individual sites or applications, no more trying to remember a fistful of different username/password combinations.

To businesses, the benefits are also compelling. First, single sign-on improves staff productivity. IS Decisions research found that complex IT security costs each individual employee 21.88 minutes every week, which equates to 182 days of lost productivity for companies of 250 people, and 21.9 days for companies with 30 people.

Single sign-on services help lower this figure, saving money for businesses. Secondly, single sign-on means fewer help requests to the IT department from users who have forgotten their login, which in turn means the IT team has more time to focus on other important work.

Such is single sign-on's popularity that around 20% of people use their social media login over traditional email and password logins for different applications.

Tom's IT Pro argues that single sign-on services are a must for large enterprises, and Business 2 Community calls it a "hot commodity for businesses".

However, while the charge to productivity is all well and good, it must not and cannot compromise security.

Anything that makes your corporate systems less safe is not worth pursuing because, at the end of the day, convenience is not more important than security.

Which is why the recent hack on password manager OneLogin is worrying. Attackers managed to obtain the login credentials of users "served by our [OneLogin's] US data centre" — and the even more worrying part of the breach is that the perpetrators have the power to crack the encrypted data they now have their hands on. This spells bad news for businesses

Why single sign-on services are now vulnerable

The implications of an attack of this kind are serious. Consider this analogy — each individual login is a troop on the frontline of security for the defence of the network. The more troops you have, the stronger that frontline is.

However, by implementing single sign on, a company effectively reduces the number of troops on the front line, rendering what's left very vulnerable.

To mix that metaphor with a simile, it's a bit like putting all your eggs in one basket.

We're not the only ones who hold this opinion. Gartner financial fraud analyst Avivah Litan agrees, saying: "It's just such a massive single point of failure.

And this breach shows that other [cloud-based single sign-on] services are vulnerable, too.

This is a big deal and it's disruptive for victim customers, because they have to now change the inner guts of their authentication systems and there's a lot of employee inconvenience while that's going on."

Single sign-on services are certainly a 'massive point of failure'. All it takes is one instance of bad user behaviour to lead to a severe breach, for example, an employee sharing a password or leaving a workstation unlocked, an employee falling victim to a phishing attack, or a malicious user stealing colleague's credentials.

The OneLogin attack has therefore cast doubt over the security of single sign-on services, and understandably, businesses who use single sign-on services are wondering how to better protect their corporate systems.

Whatever the method, the key is to protect the basket in which you've placed all your eggs.

How context-aware technology can protect single sign-on services

One way to do that is through 'context-aware' security. The trouble with passwords is that they behave exactly like keys.

As long as you have the key, you can unlock the door. Context-aware security, though, goes way beyond keys, and analyses the situation in which an access attempt takes place to determine whether the person trying to log in is exactly who they say they are.

For example, context-aware security can analyse what geographical area the login is taking place, what device the user is logging in on, what time it's happening, what the IP address is, and many other pieces of contextual information.

All of this information together builds up a profile of the person logging in, and can shed light on anything suspicious.

For example, say you restrict single sign-on logins to particular workstations, departments, devices, IP addresses, times of day or geographies, organisations can reduce the size of the opportunity for would-be attackers.

For example, if Chuck were using Larry's credentials to log in from his own desktop, and the company had restricted Larry's logins to just his own devices, Chuck wouldn't be able to gain entry.
Or if someone in one department used the credentials from someone in another department to gain entry from the wrong workstation, again, the system would deny access.

Context-aware technology has been around for a number of years but its popularity is growing considering the need to better protect logins.

Some of the most devastating security breaches recently have occurred as a direct result of compromised credentials, and with the growth of single sign-on popularity, the consequences of compromised credentials are only set to get worse.

Context-aware security, therefore, is the equivalent of changing your wicker egg basket into a virtually impenetrable thick iron box.

About the Author

François Amigorena is the founder and CEO of IS Decisions, a provider of infrastructure and security management software solutions for Microsoft Windows and Active Directory.

IS Decisions offers solutions for user-access control, file auditing, server and desktop reporting, and remote installations.

Its customers include the FBI, the United Nations and Barclays who rely on IS Decisions to prevent security breaches; ensure compliance with major regulations; such as SOX, FISMA and HIPAA; quickly respond to IT emergencies; and save time and money for the IT department.