By Kacy Zurkus, Writer, CSO | JUN 17, 2016 1:17 PM PDT

Identity: the new perimeter?

If IT can have better control over an organization's data and user identities, will they have stronger security?

Thinkstock

Organizations continue to focus the bulk of their security spending on endpoints, as well as server and network security software/solutions. Yet as organizations turn to new cloud and mobile infrastructure, they lose the control they once had over their IT assets.

If protecting the perimeter no longer provides sufficient security, then what alternatives do security practitioners have to best defend the enterprise?

For those who are new to security, you've likely been trained in user identity, access management, and behavior analytics, but knowing which tools will provide you the greatest visibility and finding the budget for those tools might be a challenge.

Being able to articulate the strength of defense that identity access management (IAM) tools provide will give you leverage in security discussions across the enterprise. Whether it is in awareness training programs with employees or budget talks with the security team, talking about how to defend against attacks on user identity via stolen credentials is now more critical than conversations about endpoint tools.

"In the age of IoT and the work from anywhere mantra where 70% of employees have substantially more access than they need, implementing an IAM solution is no longer a nice-to-have for IT departments," said Arend Verweij, CEO of IDdriven.

Organizations need to ensure that they have a clear understanding of which identities have access to sensitive data, what those identities should have access to, and whether or not they are posing risks to their organization.

What are the risks to enterprise security related to identity?

"Most of the studies show that in security breaches, 80% are the result of misused credentials. These include users that shouldn't be there anymore but are still active," said Verweij.

It's not surprising, given the fact that security teams are inundated with daily alerts, that some employees leave the company yet their user credentials don't depart along with them. "Even if you have a firewall, with credentials they can still access, so anyone who left needs to be completely removed from the system," said Verweij.

Every company should have a system in place where if you hire someone, they get access pretty quickly, but if they leave, they are kicked out of the system immediately. Verweij said he has seen far too often that removing users post departure is just not happening.

Verweij talked about a former company that he worked for several years ago in which, "We did a search for a ministry of finance for a foreign company. We found 50 accounts with direct access, but no one knew who these people were." While one might be moved to dismiss this as irrelevant because the search happened several years ago, similar searches are finding the exact same results today.

"They should have a system in place to educate people. They need to have an on-going campaign and only give certain rights and access to those who need it, **and** you need to review these controls every few months," said Verweij.

By designing and implementing these systems and practicing these habits of reviewing controls, you create an environment where it is important.

"If you don't need access to information for your job, you don't need to know. And while you don't want to create an environment of distrust, it's important to be mindful of the fact that over 30% of people are willing to sell information. That's 3 in 10 employees," said Verweij.

I know first hand that there are organizations that are not practicing these routine habits of deactivating user credentials. If an employee has been gone from a company for well over a year, why on earth is she still able to access her old email with her user credentials?