SHADOW IT – GETTING RISKIER (PART 1)

BY JAY BORDEN

Shadow IT has been around for a long time. What is it? The name represents IT services and equipment that are not maintained or monitored by the IT team and who aren't even aware they exist in many cases.

Shadow IT came about partly because servers decreased in size and price to the point where many business leaders could pay for them. They were small enough to sit under desks. Business people were trained or hired to maintain that hardware and the software running on them.

The problem was that the hardware and software were not vetted, installed, or managed by the IT organization and could pose security problems to the organization.

Shadow IT grew by leaps and bounds when Software as a Service, SaaS, became prevalent. With SaaS the hardware and software are in the cloud and maintained by the cloud service provider. No hardware or capital costs. Simple and easy and well within the budget of business leaders.

But if the hardware and software are in the cloud and maintained by the SaaS providers, how can they pose a security risk to the organization?

A good question. Many business leaders believed the cloud provider was responsible for security and the service would not pose a risk to the company.

But they do. And the risks keep growing. Why? Because to provide the service, the SaaS service typically needs access to company information. It is provided by a service account created to be used by the SaaS service and not by a person.

SHADOW IT – GETTING RISKIER (PART 1)

CONTINUED

Simple and easy. The business gets what they need. This is important. If the business doesn't have the capabilities they need, how can they sell their products or services and keep the company going?

But security is also important. It is a delicate line but one that must be considered by both sides, business and IT. The business going around IT can put the entire company at risk. IT failing to meet the needs of the business in a timely manner may jeopardize the company or push the business to shadow IT.

The risks keep growing. If one of the SaaS providers is compromised, that service account will allow attackers to access your information. Once the provider is compromised there is little between the attacker and your information.

It gets even more complex. What about demo accounts? For a service or application to be tried an account must be created with the SaaS provider and a service account to get needed information. If the decision is made not to go ahead with the SaaS service, the account with the SaaS vendor may be closed to stop billing. But was the service account created to provide needed access and information closed? In many cases this is neglected. No one is managing or protecting the access this account provides. A powerful entry point for attackers.

Think this is low probability? CISA, the federal Cybersecurity and Infrastructure Security Agency, issued a warning that Russian attackers are going after these types of forgotten accounts.

Next week we'll continue this investigation into the risks of Shadow IT.

Visit our website onebrightlycyber.com or call (888) 873-1920 to learn all the ways we help keep you safer.