Rogue Cloud Computing

The advent of cloud computing has completely overhauled the landscape of technology over the past decade. Being able to procure various infrastructures and software on a subscription basis allows companies to minimize costs and maintenance of technology assets, while gaining the flexibility to scale quickly as business grows. Consequently, these benefits drastically decreased the barrier of entry for aspiring entrepreneurs and gave rise to countless technology startups.

However, adopting a new technology is not without its risks. Leveraging cloud technology fundamentally necessitates trusting third party cloud service providers to properly store and protect your sensitive and valuable proprietary data. Indeed, major reputable cloud service providers have matured through the years and practice robust security best practices to keep your data safe from malicious hackers, but that is only one piece to the grand puzzle of your cloud security posture. Today we will be discussing a cloud security issue that is often overlooked by many companies, and that is rogue cloud computing.

Rogue cloud computing sounds pretty cool. Is it like regular cloud computing, but, like, friskier?

Rogue cloud computing, also called rogue cloud usage, occurs when a company’s business unit adopts cloud technology out of necessity or convenience, but is done without the knowledge or approval of IT. This act of bypassing unified technology management leads to a number of issues. Granted, most of these issues are not cause for concern in a lean startup, but as your business grows, they can and will amplify to greater risks if left unchecked.

Let’s walk through each of these issues with the story of a hypothetical startup called HeroGadgets. One day, Joanna from Engineering suggested to her manager Simon that since the 16-member engineering team is distributed across several time zones, they could try SlackDock, a cloud messaging service that offers group chat with mobile integration, in order to help team members easily stay connected and collaborate better. Simon liked Joanna’s idea and approved the budget for SlackDock’s lowest tiered plan, which covered up to 50 users.

So far so good, right? Well, no. According to the best practices outlined by the Control Objectives for Information and Related Technologies (COBIT) framework, onboarding of new software requires testing and certification by IT, followed by accreditation by management. Although HeroGadgets was early in its startup phase and perhaps did not need to worry about IT governance just yet, it still should have performed due diligence by verifying that SlackDock has a robust privacy policy regarding customer data, maintains a strong security posture, or at the very least, is reputable in the IT community.

A few months down the road, Sean, manager of Marketing at HeroGadgets, heard about SlackDock from a friend over beer. Sean decided his team of 8 people can really make good use of SlackDock, and signed up for their lowest tiered plan, not knowing that Engineering was already paying for the same plan with more than enough entitlements left for his team. As HeroGadgets grew in size, so did its scale of rogue cloud computing, and these cost efficiencies began to eat into its bottom line.

Friday before Thanksgiving was a bad day for John. He had been a marketing analyst at HeroGadgets for over two years, but for whatever reason, he and Sean never got along. Q3 sales numbers were dismal for HeroGadgets, and John’s head was put on the chopping block. What would John tell his family?

A distraught and bitter John returned home to find that he could no longer remotely log into HeroGadget’s network, just as he expected. But wait! While IT followed standard procedure and cut off John’s access, his SlackDock account was still alive. Upon realizing this, John downloaded his entire SlackDock chat history, including conversations useful for future litigation, and shared files containing marketing material valuable to HeroGadget’s competitors. By not having central management of cloud services, user account provisioning became a mess, and HeroGadget was exposed to risks that could have easily been prevented.

Months went by and SlackDock kept gaining popularity and expanding its userbase, attracting attention from both white hat security researchers and black hat hackers alike. One day, SlackDock announced

The unthinkable finally happened. SlackDock

A web gateway can be used to detect rogue cloud usage by monitoring outbound traffic for a list of known cloud service providers. Once the services and their respective users are identified, IT can then evaluate the associated risks and either integrate each service into their management or propose an alternative solution. User education and enforcement of relevant policies is necessary to prevent future incidents of rogue cloud usage.