Dr. A. Sperotto (UT), MASCOT

English scientific summary

Over the past decade, the trend in both the public sector and industry has been to outsource ICT to the cloud. While cost savings are often used as a rationale for outsourcing, another argument that is frequently used is that the cloud improves security. The reasoning behind this is twofold. First, cloud service providers are typically thought to have skilled staff trained in good security practices. Second, cloud providers often have a vastly distributed, highly connected network infrastructure, making them more resilient in the face of outages and denial-of-service attacks.

Yet many examples of cloud outages, often due to attacks, call into question whether outsourcing to the cloud really improves security. In this project our goal therefore is to answer two questions: 1) did the cloud make use more secure? and 2) can we provide specific security guidance to support cloud outsourcing strategies?

We will approach these questions in a multi-disciplinary fashion from a technical angle and from a business and management perspective. On the technical side, the project will focus on providing comprehensive insight into the attack surface at the network level of cloud providers and their users. We will use a measurement-based approach, leveraging large scale datasets about the Internet, both our own data (e.g. OpenINTEL1, a largescale dataset of active DNS measurements) and datasets from our long-term collaborators, such as CAIDA2 in the US (BGPStream, Network Telescope) and Saarland University in Germany (AmpPot). We will use this data to study the network infrastructure outside and within cloud environments to structurally map vulnerabilities to attacks as well as to identify security anti-patterns, where the way cloud services are managed or used introduce a weak point that attackers can target.

From a business point of view, we will investigate outsourcing strategies for both the cloud providers and their customers. For guaranteeing 100% availability, cloud service providers have to maintain additional capacity at all times. They also need to forecast capacity requirements continuously for financially profitable decisions. If the forecast is lower than the capacity needed, then the cloud is not able to deliver 100% availability in case of an attack. Conversely, if the forecast is substantially higher, the cloud service provider might not be able to make desired profits. We therefore propose to assess the risk profiles of cloud providers (how likely it is a cloud provider is under attack at a given time given the nature of its customers) using available attack data to improve the provider resilience to future attacks. From the costumer perspective, we will investigate how we can support cloud outsourcing by taking into consideration business and technical constraints. The decision to choose a cloud service provider is typically based on multiple criteria depending upon the company's needs (security and operational). We will develop decision support systems that help in mapping company needs to cloud service provider offers.

English public summary

Outsourcing to the cloud is mainstream business practice. Oft-quoted security benefits of the cloud are availability of skilled staff, bandwidth and compute power to head off attacks. Yet recent outages call these benefits into question. MASCOT will rigorously study cloud resilience and use the outcome to support security-conscious cloud strategies.

Dutch public summary

Clouddiensten zijn tegenwoordig standaard onderdeel van bedrijfsprocessen. Veelgenoemde veiligheidsvoordelen van de cloud zijn beschikbaarheid van ervaren personeel, bandbreedte en rekenkracht om aanvallen af te slaan. Recente cloudstoringen trekken dit echter in twijfel. MASCOT gaat grondig de weerbaarheid van de cloud onderzoeken, en de uitkomsten gebruiken voor écht veilige cloudstrategieën.