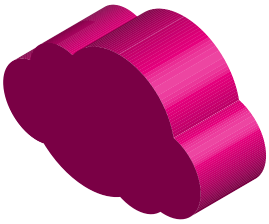
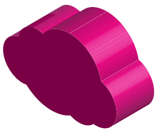
Adieu Corporate Networks?



Digitalization requires a – sometimes radical – rethinking of IT security. Is perimeter security still up-to-date for the protection of internal resources? The exploding number of smart devices and the cloud are raising doubts.



COPY —— Roger Homrich

Ja few years ago, there was a great fear of integrating mobile employees and granting them access to the intranet. How could the risks be managed when hundreds of different smartphones, laptops or pads access data and applications in the highly secured infrastructure? IT security protects the corporate network against attacks with all means at its disposal and its own employees open the door to hackers with their mobile devices. For most IT managers, Bring-your-own-device was a "red rag" alongside the cloud. Today, mobile working and cloud computing are standard.

Is it still possible to maintain the old defense concept? The perimeter security model worked well as long as all employees worked exclusively in a company's buildings and everything on the road was left out. However, with the advent of a mobile workforce, the increase in the variety of devices used, and the increasing use of cloud-based services, additional targets have emerged. "The changing environment requires consideration of existing security concepts. The previous tactic of building a corporate network that is defended like a castle with ditches, walls and drawbridges is no longer working properly," says Thomas Tschersich, Head of Internal Security & Cyber Defense at Deutsche Telekom.

OUTSIDE YOUR OWN FOUR WALLS

What's changed? So far, companies have operated IT within their corporate network – whether in their own data centers or in those of IT service providers. Everything took place at home, within one's own four walls. Anyone who wanted to enter through the door was checked, required a visa or was registered as a resident and received a permanent or temporary residence permit, for example for a specific project. Those who could not show a valid passport were not allowed through by the firewalls. But this is becoming less and less effective. Because clever attackers try to find loopholes in the corporate network and then – often undiscovered – go about their mischief. "The cost of making such a closed network secure has risen enormously in recent years. On their own, companies can no longer cope with this because the number and intelligence of attackers has increased exponentially," says Tschersich. And the security expert provocatively puts one on top: "You have to ask yourself whether a corporate network is still up-to-date from a security point of view".

Scream. Doesn't a corporate network stand for security? That's not entirely wrong, says Tschersich, but companies must face up to the fact that IT no longer has anything to do with what IT stood for ten years ago: operating proprietary software in their own data center that only their own employees were allowed to access. "Today, more and more companies are using standard software in the cloud. However, public cloud offerings cannot be operated in their own corporate network. The software is stored somewhere with the data at a provider. Far outside your own castle," says Tschersich. Employees who use this software automatically leave the corporate network. Either it goes from the office into the cloud or from the outside with the smartphone via a door into the network and at another point again from the inside through another door out of the network. "Why shouldn't we put the protection on the end device? Then we'll save all the effort for the corporate network," asks Tschersich.

IOT IS CHANGING SECURITY CONCEPTS

It is not only the classic mobile devices and the cloud that are turning the previous model of the corporate network upside down. The soaring number of networked devices in the Internet of Things will require new security approaches.

Even the networked car. They all send data to the intranet and the cloud. They have to get in and out of the network first. The cost of shielding the corporate network will continue to rise as a result.

Edge computing also sparks new challenges, shifting the analysis of data to the edge of the network or even to the outside. And that complicates things. A single smart device can create an encrypted VPN connection to the corporate network. For more complex systems, however, companies must use and manage specialized routers, routing switches, integrated access devices, multiplexers and SD-WAN solutions. The complexity of one's own network increases enormously.

So how can a company continue to ensure protection when the boundaries between the private and business networks have shifted? Are there alternatives? "There are," says the head of internal telecom security. "End devices can be protected with security software". Which apparently not everyone knows, because according to a survey by IDC, inadequately or inadequately secured end devices are among the top security risks in companies in Germany. "Those responsible for security still have a lot to do here. But there are solutions on the market. And of course it is important to actively manage the end devices. This includes installing updates centrally or preventing Shadow IT in the form of apps. But this is not new, it simply has to be implemented consistently," says Tschersich.

AT GOOGLE ONLY THE DEVICE COUNTS

Google is a prominent example of a farewell to the corporate network. Access to internal IT depends solely on the credentials of the device and the user. A user's network location is less important – whether it's a corporate location, a home network, a hotel or a café. All access to corporate resources is fully authenticated, authorized and encrypted based on device status and user data.

Google uses the concept of the Managed Device. The company procures and actively manages each device. Only these devices can access enterprise applications. A device tracking and procurement process that revolves around a device inventory database is a cornerstone of this model. All managed devices must be uniquely identified. They refer to a record in the Device Inventory Database. One way of unique identification is a device-specific certificate. To obtain a certificate, a device must be present and certified in the database. The certificates are stored in a certificate store. After installation, the certificate is used in all communications with enterprise services.

"The Google model has a further advantage for the security departments," explains Tschersich and knows from his own experience what he is talking about. "We security departments are going to get a little far out of our prohibitive role and instead play an active role in digitization."

✉ Thomas.Tschersich@telekom.de
www.t-systems.com/solutions/security

For many companies, the bill of securing their corporate network like a castle with ditches, walls and drawbridges no longer works.

Illustration: freepik.com