

Shadow IoT: Only 50 percent of companies know the number of their assets

Results of a major survey conducted by Armis for the DACH region indicate that decision makers should focus on simple total asset management solutions

MUNICH, GERMANY, December 16, 2021 /EINPresswire.com/ -- [Armis](#), the leading unified asset visibility and security platform provider, announces the results of a survey for the DACH region conducted in September. The results highlight that too few decision makers have an overview of all IoT

devices and do not have appropriate measures in place for detection and classification. In the DACH region, less than half of the 1,305 respondents say they know the exact number of IoT devices they use (45% each in Germany (DE) and Austria (AT), 44% in Switzerland (CH)).

When it comes to assessing the risk of undetected devices, minds are divided. The number of respondents who assess the risk as low is roughly equal to the number who assess the risk as high (36% each in DE, 37% and 38% in AT, 35% and 38% in CH). The remaining participants are not concerned about this or are unable to make a statement.

Nevertheless, in the question that follows, the majority consider it likely or very likely that their devices forward data via the Internet and that their devices and thus also their data can be accessed (65% in DE, 72% in AT and 74% in CH). However, about half of the respondents in Germany and Austria (46% and 48%) would be reluctant to give up IoT devices in favor of greater data security, and 41% in Switzerland.

Only about half of the survey participants in Germany and Austria are certain that all smart devices are covered in their company (51% in DE, 53% in AT); in Switzerland, 46% are certain. The rest suspect some coverage gaps. For less than half of the respondents, [unrecorded IoT devices pose a risk to IT security](#) (42% in DE, 43% in AT and 37% in CH).

Only 14 percent of respondents from Germany and Austria are aware of commercial application



platforms for detecting and classifying IoT, compared to 12 percent in Switzerland. In Austria and Switzerland, more than half (54% and 51%), and 44 percent in Germany, assume that a manual search for undiscovered devices by a competent IT team is necessary.

"Undiscovered IoT devices pose a security risk to any organization because they communicate over the Internet, creating an unknown gateway for intrusion. IT departments must therefore also detect these devices and classify them accordingly, because only the [complete capture of all assets](#) provides the basis for successful risk management," said Alexander Bünning, Regional Director DACH at Armis. "However, IT departments cannot do this detection manually. There are too many devices with potentially unknown vulnerabilities, so they should rely on automated technologies. Decision makers can mitigate risk by giving their IT departments the right tools," Bünning concludes.

The online survey, conducted by YouGov Deutschland GmbH, polled people who work in at least middle management and/or IT. A total of 1,305 people were surveyed, 505 of them in Germany, and 400 each in Austria and Switzerland. The survey took place between Sept. 08 and Sept. 17, 2021.

About Armis

Armis is the leading unified asset visibility & security platform designed to address the emerging threat landscape of connected devices. Numerous organizations worldwide rely on Armis' real-time, continuous protection to provide full contextual visibility of all managed, unmanaged and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management and automated policy enforcement. Armis is a privately held company headquartered in Palo Alto, Calif.

Bastian

Armis

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

[Other](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/558498009>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2021 IPD Group, Inc. All Right Reserved.