IDC INFOBRIEF SHOWS HOW IT SECURITY PREPARES COMPANIES FOR THE FUTURE

Learn more here

The "new normal" has massively changed the perception of IT security inside companies. A LastPass/IDC Info Letter shows how IT security makes companies ready for the future.

The "new normal" and remote work have caused for extensive change. Top of the list: The perception of IT security within companies has proven to be one of the main pillars when it comes to creating the right setup for remote working teams.

Secure Remote-Work and seamless user

A key role for identity and access management

IDC and LastPass have created a detailed Inforbrief on this, and the outcome is highly convincing: Modern identity and access management enables convenient, seamless and efficient work with a vast variety of devices and from varying locations without undermining high corporate security standards. Identity and access management and the use of a password manager – these are measures that fulfill the requirements of all stakeholders. This is how IT security manages to meet the security demands imposed by remote working while still ensuring a good, seamless user experience.

The security experts of LastPass advise companies to consider the following steps:

1 Use of single sign-on

SSO provides the IT system with full control and simplifies access administration. It enables a seamless user experience without reducing IT transparency and control.

2 Introducing multifactor authentication

By using biometric data MFA creates an additional security level for companies and a positive user experience, e.g. password-free log-in (Note: 60% of MFA-users confirm that MFA contributes more security to the organization)

3 Use contextual factors

Using contextual factors such as localization or IP addresses offers the IT system additional control and security by considering the plausibility of the sign-in situation (time, place, device).

4 Securing the VPN

Strong passwords and MFA on the VPN ensure that the people signing in actually are who they claim to be – before they get access.

5 Protecting workstations

MFA for workstations ensures that only legitimized persons are able to authenticate themselves (e.g. by using biometric or contextual factors).

6 Securely share

Password sharing ensures that all staff have access to the data they require for their work.

7 Reducing passwords

Password-free authentication eliminates passwords from the log-in process and ensures a seamless user experience.

8 Tackle "shadow IT"

A password manager offers employees a secure location to store all their credentials – the ones IT does and does not know about.

9 Preventing phishing patterns

Password management can help to reduce the risk of phishing by never executing actions on suspicious sites.

10 Maintaining an overview

Detailed reports provide an overview across all activities and enable adjustments of access and authentication where necessary.

A new perception of IT security

It is much more than a side effect that in this context IT security is able to position itself much more strongly in the view of management, too. IAM will help to strengthen the role of IT in the long term – and this is something all stakeholders will benefit from. Check out the Infobrief, it's well worth reading!

Barry McMahon, Senior Manager IAM,
LastPass by LogMeIn

LastPass •••|
by LogMeIn