How delaware can help you to optimize your cloud security

delaware has multiple security offerings, to support its customers with an approach that is tailored to their needs. One of our most popular offerings, is the Microsoft 365 security analysis and advisory.

FOR WHOM?

- Organizations with an Office 365 or Microsoft 365 license that want to improve their security.
- Organizations using SharePoint online, Exchange online, Microsoft 365, …

WHAT?

- Security presentation to make you aware about the different security features
- Security analysis of your current environment. (Assessment and threat check)
- Advising and designing a roadmap for short-, medium- and long-term security projects.

BENEFITS

- Get an security overview of your environment and detect possibilities to improve security.
- Increase the security of your organization.
- Having access to a partner who is eager to assist you.

We do an analysis and offer you advice

- Pre-Engagement
  - Define scope and align expectations to guide workshop and deliverables.
  - Threat Check and Assessment
- Discover threats in your Microsoft 365 cloud environment by enabling our analyzing tools
  - Review the environment based on Microsoft best practices
  - Determine risks and the maturity of your current Microsoft 365 security environment.
  - Identify unused security features included in the current license bundle.
- Workshop
  - Raise awareness of available Microsoft 365 security features.
  - Determine your security needs
  - Present the threat check and assessment report
  - Demo the preferred features
  - Discuss a possible roadmap for quick wins and short-, medium- and long-term improvements.

Because the security offerings, features and threats are constantly changing, recurrent sessions can be organized.

What is included:

- Threat analyzing
- Assessment
- Awareness workshop
- Assessments and threat analysis report presentation
- Presentation and definition of next steps (roadmap)

###

We often notice recurring concerns from our customers. That's why the issues below are always checked and discussed during our assessment.

- **Review access of internal and external users**

With Microsoft cloud, you can easily collaborate both within your organization and with users from external organizations, such as partner companies. Users can join groups, invite guests, connect to cloud apps, and work remotely from their business or personal devices. Unfortunately, it is easy to lose track of all these users, specifically of external users. Without a clear overview, you won't know which users still need access or which accounts are unused and can be deleted. With Azure AD, you can review and track access for internal and external users.

- **Block files before an end-user can open it (via email, SharePoint, Teams,…)**

As email is still the most used system to spread malicious files, it should be protected in the cloud. A company's IT team however has little or no control over external devices accessing company email, something that has become commonplace – even essential – in modern businesses. Mobile-first is the future, but it makes companies very vulnerable for security problems.

When you access your work email using your Android smartphone, do you worry about how protected it is? Probably not. The solution is to apply security measures that are active between the device and the cloud. Luckily, Microsoft offers a solution that scans emails, Teams content and SharePoint for malicious files.

- **Privileged accounts are the main target – reduce the amount of privileged accounts**

A privileged user with administrator rights for instance, can be compromised because of one small mistake. A company should minimize the number of people who have access to secure information or resources, as this reduces the chance of a malicious actor getting that access, or an authorized user inadvertently impacting a sensitive resource. However, users still need to carry out privileged operations in Azure AD, Azure, Office 365, or SaaS apps. One of the solutions for this issue is to give users just-in-time (JIT) privileged access to Azure resources and Azure AD.

###

Would you like to optimize your cloud security, but this isn't completely what you're looking for? No worries, delaware has a broad array of security solutions:

- Embed security from the start – Into the development process: DevSecOps: shift security left
- Safeguard what you've built, managed by accredited security experts: Managed Security Services
- Improve user experience by providing staff with secured and well-managed mobile devices: Managed mobile devices

Working with an experienced cloud security partner like delaware offers important added advantages and can ensure the security of your cloud-based business environment. Don't hesitate and get in touch today! Reach out to your delaware contactperson or to Maarten Leyman, cloud enablement and operations team lead at delaware.

###