Practical Assessment: DLP

An emergency executive meeting at Oscorp was held after reports of serious side effects of Oscorp's new medication hit the press.

Norman Osborn and Harry Osborn are extremely concerned. They suspect an employee has leaked the information to the press.

Oscorp use Microsoft Office 365 and The Microsoft Azure cloud. Internally, they use Microsoft SharePoint.

Problem: Oscorp wants you to design a comprehensive "Insider Threat" program to monitor and stop employees from stealing and leaking sensitive data outside the organisation.

sensitive data outside the organisation.

Your answer

We want to check whether Oscorp has DLP in place to avaoid exfiltration. We also want to check the network infrastructure of Oscorp if there are perimeter firewalls installed and how

do they respond. We would also want to know if Oscorp protects its documents with passwords as as per the NIST framework. We also want to make sure if Oscorp has a data classification policy and whether they have a procedure to label or tag data for DLP to be effective. We want to know if Oscorp uses AD for authentication of who can access data. We want to know if Oscorp has too many admin accounts on the AD side and whether they use Privilege access management tools to keep an eagle eye view there. We want to know if correct encryption methods are in place to protect Oscorp's data from being read or hacked easily

The first step in establishing an effective Insider Threat program is to ensure that identity and access management (IAM) is managed properly, which we covered in practical assessment of the previous module.

Therefore, our focus here will be on DLP and data security measurements.

The first step, which is a low-hanging fruit would be to block access to any USB flash drives. Simply stopping employees from copying data to external USB flash drives and hard drives is a simple yet effective control measures that's technically free to implement.

The next step would be to undertake a data discovery activity to ensure that the cyber security team have visibility over all data, specially sensitive data. Since this is an urgent undertaking, the focus should be on data related to Oscorp's controversial drug. We know from previous assessments that the formula is stored on a Microsoft SQL database so that would be our first location.

Next, a search through Microsoft SharePoint to discover any files related to the drug.

Finally, tag and label all data related to the drug as Highly Sensitive using Microsoft Azure AIP.

Since Oscorp uses Microsoft products, then a DLP solution from Microsoft is probably the most cost effective and easiest to implement. If you do a research, you will find that this product from Microsoft can do the trick.

Configure Strict DLP rules to prevent sending or copying any files tagged as "Highly Sensitive".

Finally, conduct a physical search on desks to try and find any physical files related to the drug. They should all be kept in a secure file cabinet to reduce the risk of employees taking photos of sensitive files using their phones.

Recommendations:

GRC Mastery by Abed Hamdan