OZON Security Excercise

THIS PAGE IS PART OF THE OZON Security Exercise. THIS MEANS THAT ANY INFORMATION PRESENTED HERE IS A TEST AND NOT A TRUE REPRESENTATION OF THE REAL WORLD.

The Netherlands IT infrastructure is currently under attack and we also are experiencing hacking attacks due to a flood of published vulnerabilities in different packages. Below we describe actions taken to mitigate the effect of these attacks and vulnerabilities on our systems.

Date: 23 March, 2023	
Time	**Description**
13:15	Openssh has a vulneraibility, we have to close all ssh access to the systems for now. Please use our VPN to access our systems from remote
12:35	Similar to the Dymo label printers several of our HP Printers have a firmware bug that requires us to shut them down until a firmware patch is available
12:10	Due to a new vulnerability in the owncloud server software for which a patch is not yet available, the owncloud server has been temporarily shutdown
11:30	We are sorry to inform you that due to a still unknown reason all our passwords have been taken and published on the WEB. Therefore, you need to change your password asap.
10:50	A vulnerability in several lab equipment software has been revealed. The Lab coordinators have been informed to disconnect any of the affected systems
10:30	It is better to refrain from running Teams Meetings until vulnerability is resolved. We advice you to use zoom for now
10:18	Several security vulnerabilities in MSTeams have been revealed. You are advised to not run MS Teams via Wireless network, but use the cabled network
09:50	We detached all Dymo label printers and have taken them back to the IT department to initiate firmware update process to fix a vulnerability issue
09:30	Due to a vulnerability in the security CERT key handling software it is possible that what seems to be a secure connection, for instance the green lock on a website, may not be secure. So please inspect the the website addresses. Additional warning about phishing emails, please inform us if you have any trouble with 2FA - in fact report any secure connection trouble

From:

https://helpdesk.strw.leidenuniv.nl/wiki/ - **Computer Documentation Wiki**

Permanent link:

https://helpdesk.strw.leidenuniv.nl/wiki/doku.php?id=ozonsecurityexercise

Last update: **2023/03/24 08:04**