WEEKLY BULLETIN

3-7 JULY 2023

Quote of the week

To competently perform a security correction service, two critical elements of incident response are necessary: information and organization."

Content:

- Cyber security in the health sector. Valuable advice
- Continuous meetings of AKCESK with Critical Information Infrastructures on increasing vigilance and strengthening security measures

Cyber security in the health sector. Valuable advice

"Other industries may rely more on security by isolating sensitive data so it's not connected to the Internet, but that's not the case for modern healthcare."

Christopher Porter – Head of Threat Intelligence at Google Cloud

1: Train employees on data security

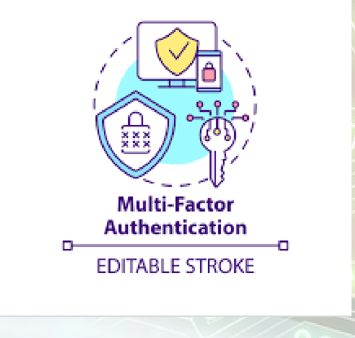
Training your employees on the importance of data security, data protection policies and the consequences of a data breach can help ensure that healthcare data remains confidential and secure. Giving employees the tools and knowledge they need to recognize and respond to potential security threats can help mitigate any risk, and it's not something to be taken lightly.

2: Conduct risk assessments routinely

Regular risk assessments are essential to protect data, not just healthcare data. It is important to take the time to review and audit healthcare systems, databases and network security to identify potential security risks and ensure that all necessary measures are in place to mitigate those risks.

3: Multi-Factor Authentication (MFA)

MFA adds an extra layer of security by requiring additional verification in addition to a username and password. MFA can dramatically reduce the risk of data loss or unauthorized access and is an absolute must for organizations dealing with sensitive healthcare information.



Auditing & Monitoring

Auditing and monitoring involves detecting, analyzing and responding to potential security events within healthcare systems. This includes examining user access to sensitive data and verifying the accuracy of stored data

Continuous meetings of AKCESK with Critical Information Infrastructures on increasing vigilance and strengthening security measures

In the framework of raising awareness of critical and important information infrastructures, the National Authority for Electronic Certification and Cyber Security, in continuation of previous meetings, has organized a series of meetings today with all sectors to increase vigilance and strengthen measures of cyber security in their infrastructures and to discuss the possible problems in these sectors.

The meeting emphasized the importance of sharing information in real time, in order to distribute appropriate measures to all other infrastructures to create a cyber environment as safe as possible.

WEEKLY BULLETIN

3-7 JULY 2023

Quote of the week

To competently perform a security correction service, two critical elements of incident response are necessary: information and organization."

Content:

The European Union Agency for Cyber Security (ENISA) publishes its first cyber threat landscape report for the health sector.

The European Union Agency for Cyber Security (ENISA) recently published its first cyber threat landscape report for the health sector. The report identifies the main threats, threat actors, trends and covers a period of over 2 years. The document also analyzes the impact of cyber attacks on the sector and provides details about the entities and assets most targeted. The study is based on a total of 215 publicly reported incidents in the EU and neighboring countries.

According to the report, organizations in the European healthcare sector experienced a significant number of incidents, with healthcare providers accounting for 53% of total incidents, 42% of reported incidents targeting hospitals, while health authorities, bodies and agencies accounted for 14% and finally the pharmaceutical industry 9%.

The report further highlights the financial implications, revealing that the average cost of a significant security incident in the health sector is estimated at €300,000, as shown by the "ENISA NIS Investment 2022" study.

Read more

2 Android Apps Collecting Private Data Without Authorization are Discovered.

Two Apps on the Google Play Store were recently discovered to be spyware that sent the private data of 1.5 million users to suspicious servers in China.

According to a report by a mobile security company the 2 apps include: File Recovery and Data Recovery with over 1 million installs and File Manager with over 500,000 installs

The stolen data includes contact list, audio, photo, video, real-time location, mobile operator and mobile device data.

As a user, it is imperative that you remain vigilant, show caution when downloading apps, and rely on safe sources to download these apps to your devices.

Read more

Microsoft denies the stealing of 30 million customer accounts

Microsoft has denied claims by so-called "Anonymous Sudan" hacktivists that they breached the company's servers and stole credentials for 30 million customer accounts.

Last month, Microsoft admitted that Anonymous Sudan was responsible for service outages in early June that affected several of its services, including Azure, Outlook and OneDrive.

The hackers claimed that they had "successfully hacked Microsoft" and "accessed a large database containing more than 30 million Microsoft accounts, emails and passwords".

Anonymous Sudan offered to sell this database to interested parties for $50,000

It is currently unclear whether Microsoft's investigation has ended or is ongoing. Also, the company's reaction to the possible public release of the data remains to be seen.

Read more

PATCHING ALERT

Android security updates fix three actively exploited bugs

Google has released its monthly security updates for the Android operating system, which come with fixes for 46 vulnerabilities.

The most serious security issue that Google fixed this month is CVE-2023-21250, a critical vulnerability in the Android System component that affects Android versions 11, 12, and 13.

Exploitation of CVE-2023-21250 could lead to remote code execution without user interaction or additional execution privileges

This month's Android security update covers Android versions 11, 12 and 13, but depending on the scope of the vulnerabilities addressed, they may affect older versions of the OS that are no longer supported.

It would be advisable to replace your device with a newer model or install a third-party Android distribution that applies security updates to older devices, albeit with a delay.

Read more