HealthManagement
Promoting Management and Leadership

Cyber-Attack Protocols A Must As German Hospital Shut Down By Malware

German Hospital shut down by Malware; Reporting Protocols a MUST!

A cyber-attack that brought an almost fully paperless hospital in Germany to a standstill, has raised serious concerns about the lack of pan-European reporting protocols when dealing with such malicious viruses.

This has prompted the European Association of Healthcare IT Managers (www.hitm.org) to take the initiative and draft procedural protocols for discussion and adoption with stakeholders, as the wider health sector is seen as being extremely vulnerable to such cyber-attacks.

The IT systems of Lukas Hospital in Neuss, North Rhine-Westphalia, was infected by a virus in the middle of last week, which experts said had been sent as an email attachment and probably opened by mistake.

While initially, hospital spokesman Dr. Andreas Kremer explained that it would likely take until the end of last week for IT experts to remove malicious software, today the hospital was still offline. The facility website still requests contact by phone and fax only.

“We are in the process of restoring all systems back to normal,” Dr. Kremer told the leading industry magazine *HealthManagement.org* on Tuesday.

The problem was first noticed by staff of the 540-bed facility who spotted errors and delays in the system. Finally, access to all electronic medical records (EMR) data was locked by what seems to be a ‘ransomware’ virus.

After the attack the hospital confirmed in a statement that the cause for the breakdown was a malicious virus sent from an unknown source, but added that the action did not appear to be targeted, as there was no blackmail attempt.

IT systems were immediately shut down to protect sensitive patient data. Kremer said that owing to encryption and routine updates prior to the attack, all patient information was secure. Doctors and patients were informed about the system failure by leaflet.

Following the attack, staff could carry out 80 percent of surgeries, while non-urgent cases got rescheduled, and severe ED cases were transferred to other hospitals.

“A serious worry seems to be the lack of clear criteria in IT security law for reporting on cyber attacks. Lukas Hospital has done here a courageous step forward to inform immediately the public. This transparency reassures trust in the institution and helps to counter future attacks much more easily,” said Christian Marolt, Secretary General of the European Association of Healthcare IT Managers.

According to the German daily *Westdeutsche Allgemeine Zeitung,* two other hospitals and a company in North Rhine-Westphalia have also been affected by the virus in recent weeks but the incidents have not been made public. In such context serious questions have to be asked: how many companies in Europe apply “strict secrecy” over cyber attacks and cover them up? And how many of them pay ransom? And how many hide financial losses cleverly in their balance sheet?

Lukas Hospital, which has been almost paperless for over a decade and - according to the “FOCUS Hospital Report” - one of the best clinics in Germany, has called for the support of top IT experts from Germany and the UK to get the problem under control. Kremer explained that they were working to decode the virus which rapidly evolves and changes its details almost hourly but it will take at least until the weekend until the almost 1,000 PCs are fully back at work.

“The financial loss caused by the virus will not be ascertained until the facility is up and running fully again. Each day when our operation is at a standstill, ensures that revenues will be lost,” Kremer concluded.

Sources:

Lukas Hospital, Dr. Andreas Kremer

Westdeutsche Allgemeine Zeitung

Published on : Tue, 16 Feb 2016