

Virus cripples Royal Melbourne Hospital Pathology - blueAPACHE

Canonical:

<https://www.blueapache.com/blog/virus-hits-royal-melbourne-hospital-and-its-not-the-type-they-normally-see>

Details:

Summary

This blueAPACHE post reports: Royal Melbourne Hospital has been targeted by a hack that has significantly impacted their IT systems, and in turn, the services they can provide to those most in need. Melbourne Health, the network which runs the hospital, are currently attempting to identify the virus and restore operations. It concerns emPOWER Core Network & Data Centre Interconnect, emPOWER Connectivity, emPOWER Security. It names Microsoft in connection with the announcement. Published in 2016. Figures, product names and event details reflect that time; for current information see the linked service pages.

Key facts

Label	Value
Publication year	2016
Services referenced	emPOWER Core Network & Data Centre Interconnect, emPOWER Connectivity, emPOWER Security
Named products or vendors	Microsoft

Article

Royal Melbourne Hospital has been targeted by a hack that has significantly impacted their IT systems, and in turn, the services they can provide to those most in need. Melbourne Health, the network which runs the hospital, are currently attempting to identify the virus and restore operations. Melbourne Health is one of Victoria's largest hospital networks and includes a rehabilitation centre and mental health service. The virus has infected Windows XP computers within Melbourne Health's Pathology department. Microsoft ceased support and security updates for the obsolete operating system on April 8, 2014. Continuing to run critical services on an unsupported operating system, especially those that directly impact patient health and operations, carries an extreme risk. Without the regular security patches and updates from Microsoft, the operating system becomes a playground for hackers to exploit. Staff at the pathology department are now manually processing blood, tissue and urine samples instead of leveraging their systems to register, test, record and communicate results. Only urgent pathology specimens are being processed due to delays resulting from the manual workarounds. Staff are being encouraged to use fax to communicate the need for urgent results, while critically abnormal results are being phoned to wards (including intensive care and the emergency ward). Associate Professor Denise Heinjus, Executive Director Nursing Services and Allied Health sent an email Monday afternoon to staff explaining:

Melbourne Health's IT department is implementing a network-wide solution to the virus and a solution may take some time.

The hospital's food service was working with nurses to ensure that the right meals continue to be delivered to the right patients.

Payroll had not been affected by the virus.

Through manual work-arounds, staff had been able to minimise disruption to patients so far.

A spokeswoman stated that "patient safety has always been our highest priority and has been maintained... Elective surgeries and outpatient appointments are continuing as normal.

"We are working to fix this issue as quickly as possible. As soon as the virus has been removed, we will investigate how it came to infect Melbourne Health." When asked if the virus would jeopardise the safety and privacy of patient's records, she made no comment. The spokeswoman declined to say when the virus was first detected and how long it was likely to cause problems for. She also would not comment on whether patients and ambulances should avoid the hospital's emergency department. As we become more globally connected, the importance of maintaining IT systems increases. This isn't a new thing, it has been very apparent since we welcomed the internet into our operations. And while it has been traditionally cost-prohibitive to roll-out and support new desktops across an organisation, there are IT as a Service (ITaaS) and Desktop as a Service (DaaS) options that can mitigate the capital investment, removing these barriers. The excuses for not maintaining systems and inadvertently creating high risk IT environments are simply no longer valid. As much of the health sector relies on block funding that is subject to service delivery capability, it will be interesting to see the true impact this virus has. To learn more about ITaaS and DaaS, or better understand your risk profile, contact the blueAPACHE Consulting team .

Related

emPOWER Core Network & Data Centre Interconnect

emPOWER Connectivity (pillar)

emPOWER Security

emPOWER Security (pillar)

Frequently asked questions

Which department at Royal Melbourne Hospital was infected by the virus, according to the article?

The article says the virus infected Windows XP computers within Melbourne Health's Pathology department.

When did Microsoft cease support for Windows XP, according to the article?

The article says Microsoft ceased support and security updates for Windows XP on 8 April 2014.

What manual workarounds does the article say pathology staff adopted?

The article says staff began manually processing blood, tissue and urine samples, prioritising only urgent specimens, using fax to communicate urgent results, and phoning critically abnormal results to wards including intensive care and the emergency ward.

What did the Melbourne Health spokeswoman say about patient safety, according to the article?

The spokeswoman said patient safety had always been the highest priority and had been maintained, with elective surgeries and outpatient appointments continuing as normal.

Is the information in this post still current?

No. It reports a specific 2016 hospital IT incident; for blueAPACHE's current security and managed services, see the emPOWER Security pillar page rather than this post.

Source

<https://www.blueapache.com/blog/virus-hits-royal-melbourne-hospital-and-its-not-the-type-they-normal-y-see/>

Knowledge Base

What incident does the blueAPACHE blog post 'Virus cripples Royal Melbourne Hospital Pathology' describe?

a hack/virus that targeted Royal Melbourne Hospital, significantly impacting Melbourne Health's IT systems and, in turn, the services the hospital could provide to patients.

Which hospital department was infected by the virus, and what type of computers were affected?

The virus infected Windows XP computers within Melbourne Health's Pathology department.

Why was running Windows XP considered a major risk in this incident?

Microsoft ceased support and security updates for Windows XP on April 8, 2014, so continuing to run critical services on the unsupported operating system left it without regular security patches, making it a playground for hackers to exploit — an extreme risk for services impacting patient health and operations.

How did pathology staff cope with the systems outage?

Staff manually processed blood, tissue and urine samples instead of using their systems to register, test, record and communicate results. Only urgent pathology specimens were processed due to delays from the manual workarounds, staff used fax to communicate urgent result needs, and critically abnormal results were phoned to wards including intensive care and the emergency ward.

What did Associate Professor Denise Heinjus communicate to staff about the incident?

Associate Professor Denise Heinjus, Executive Director Nursing Services and Allied Health, sent an email explaining that Melbourne Health's IT department was implementing a network-wide solution (which might take time), that the hospital's food service was working with nurses to ensure correct meals were delivered to the right patients, that payroll had not been affected by the virus, and that manual workarounds had so far minimised disruption to patients.

What did the hospital spokeswoman say about patient safety and the investigation into the virus?

The spokeswoman stated that patient safety had always been the highest priority and had been maintained, that elective surgeries and outpatient appointments were continuing as normal, and that they were working to fix the issue as quickly as possible and would investigate how the virus infected Melbourne Health once it was removed.

Did the hospital spokeswoman comment on patient record privacy or emergency department safety?

No. When asked if the virus would jeopardise the safety and privacy of patients' records, she made no comment, declined to say when the virus was first detected or how long it would cause problems, and would not comment on whether patients and ambulances should avoid the hospital's emergency department.

What solution do you suggest to prevent organizations from running high-risk, unmaintained IT systems like the one at Royal Melbourne Hospital?

We suggest that IT as a Service (ITaaS) and Desktop as a Service (DaaS) options can mitigate the capital investment traditionally required to roll out and support new desktops, removing the cost-prohibitive barriers and eliminating excuses for not maintaining systems and inadvertently creating high-risk IT environments.

How can readers learn more about ITaaS and DaaS or assess their own IT risk profile ?

The article invites readers to contact our Consulting team to learn more about ITaaS and DaaS or to better understand their risk profile.