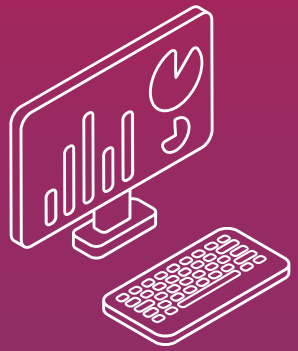
THE IMPORTANCE OF CYBERSECURITY IN HEALTHCARE



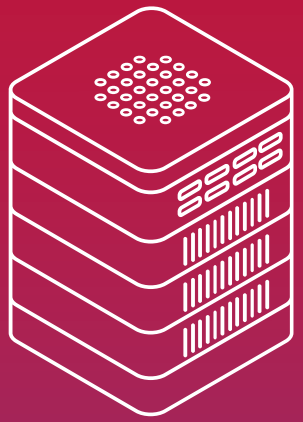
UNIT TEKNOLOGI MAKLUMAT
HOSPITAL KAJANG
SEPTEMBER 2024

Pengenalan Cybersecurity dalam Healthcare

- Dalam sektor kesihatan, keselamatan siber adalah sangat penting untuk melindungi maklumat pesakit yang sensitif.
- Dengan penggunaan sistem digital yang meningkat, memahami kepentingan kawal selia keselamatan siber seperti Personal Data Protection Act (PDPA) adalah penting.

Overview keselamatan siber (*cybersecurity*)

- Keselamatan siber (*cybersecurity*) ialah perlindungan sistem komputer, rangkaian dan data daripada akses dan serangan yang tidak dibenarkan.
- Dalam perlindungan kesihatan (*healthcare*), kepentingannya tinggi kerana maklumat pesakit adalah sulit, menjadikan langkah keselamatan siber yang teguh amat diperlukan dalam mencegah pencerobohan dan mengekalkan integriti maklumat.



Kepentingan Keselamatan Siber untuk Data Pesakit

- Pelanggaran data dalam perlindungan kesihatan boleh membawa kepada akibat yang teruk, termasuk kecurian identiti dan penipuan kewangan.
- Melindungi data pesakit bukan sahaja mematuhi peraturan tetapi juga memelihara integriti dan kerahsiaan maklumat kesihatan, mempromosikan keselamatan dan kepercayaan pesakit dalam sistem perlindungan kesihatan.

Personal Data Protection Act (PDPA) 2010

- PDPA 2010 mengawal selia pemprosesan data peribadi di Malaysia.
- Ia menetapkan garis panduan untuk perlindungan data
- memastikan maklumat pesakit dikendalikan dengan berhati-hati
- mempertahankan hak privasi individu dan memperkukuh amalan keselamatan siber dalam perlindungan kesihatan.

Memahami Ancaman Siber

- Sistem perlindungan kesihatan menghadapi pelbagai ancaman siber yang boleh menjejaskan data pesakit dan mengganggu perkhidmatan.
- Memahami ancaman ini adalah penting untuk membangunkan strategi keselamatan yang berkesan.

Ancaman siber dalam perlindungan kesihatan

- Organisasi perlindungan kesihatan terdedah kepada pelbagai ancaman siber termasuk serangan pancingan data (*phishing attacks*), ransomware, pelanggaran data dan kejuruteraan sosial.
- Ancaman ini boleh membawa kepada akses tanpa kebenaran kepada maklumat pesakit yang sensitif dan kurugian kewangan yang ketara.

Serangan Phishing

- Serangan pancingan data (*phishing*) ialah ancaman yang lazim dalam perlindungan kesihatan, di mana penyerang sering menyamar sebagai organisasi yang sah untuk mendapatkan maklumat sensitif.
- Serangan ini boleh menyebabkan kecurian *credential* dan akses tanpa kebenaran kepada rekod pesakit

Insiden *Ransomware*

- Insiden perisian tebusan (*ransomware*) telah melonjak dalam perlindungan kesihatan, sering menyulitkan data (data *encrypting*) kritikal untuk menuntut bayaran untuk penyahsulitan (*decryption*).
- Pada tahun 2020 sahaja, 34% organisasi perlindungan kesihatan melaporkan mengalami serangan perisian tebusan, menjelaskan perlindungan pesakit dan kestabilan kewangan.

Pelanggaran Data

- Pelanggaran data adalah sangat membimbangkan, dengan perlindungan kesihatan menjadi sektor yang paling disasarkan.
- Pada 2021, lebih 45 juta rekod pesakit telah didedahkan di A.S., menekankan keperluan langkah keselamatan siber yang teguh.

Teknik kejuruteraan sosial

- Memanipulasi individu untuk mendedahkan maklumat sulit.
- Taktik yang digunakan termasuk berpura-pura dan mengumpan, yang mengeksploitasi psikologi manusia untuk memintas kawalan keselamatan teknikal.

Melindungi Data Pesakit

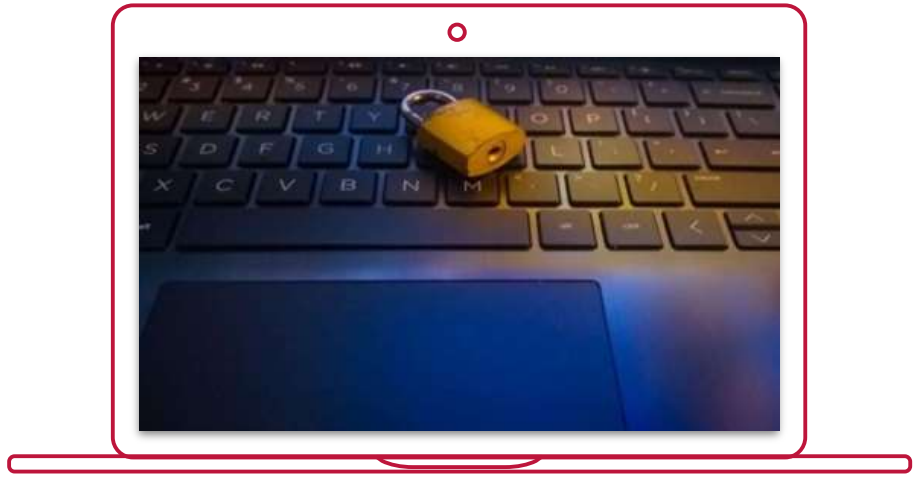
- Data pesakit semakin berisiko, memerlukan langkah perlindungan yang ketat.
- Memahami *Protected Health Information* (PHI), peranan penyulitan (*the role of encryption*), kaedah pemindahan data dan amalan terbaik adalah penting untuk memastikan privasi data dan mencegah pelanggaran.

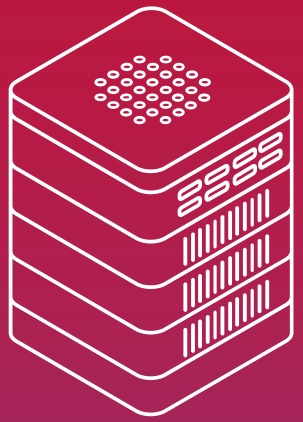
Apakah itu PHI?

- *Protected Health Information* (PHI) merujuk kepada sebarang maklumat kesihatan yang boleh dikenal pasti secara individu yang dipegang oleh penyedia perlindungan kesihatan.
- Ini termasuk data seperti nama, rekod perubatan dan maklumat pengebilan yang berkaitan dengan status kesihatan atau perlindungan individu,

Kepentingan Penyulitan (*Encryption*)

- Penyulitan (*encryption*) mengubah data menjadi format berkod, menjadikannya tidak boleh diakses tanpa kunci penyahsulitan (*decryption*) yang betul.
- Ia melindungi maklumat pesakit sensitif semasa penyimpanan dan penghantaran.
- Dapat mengurangkan risiko akses tanpa kebenaran dan pelanggaran data.





Teknik Pemindahan Data Selamat

- Apabila memindahkan data pesakit, penggunaaan kaedah selamat seperti *Virtual Private Network* (VPN), Secure File Transfer Protocols (SFTP) dan e-mel yang disulitkan (encrypted) dapat memastikan data kekal sulit semasa transit antara rangkaian dan peranti.

Amalan Terbaik Pengendalian Data

Melaksanakan amalan terbaik dalam pengendalian data termasuk:

- latihan tetap untuk kakitangan mengenai dasar perlindungan data;
- menghadkan akses kepada PHI berdasarkan keperluan; dan
- menggunakan penyelesaian storan selamat seperti pangkalan data yang disulitkan (*encrypted*) untuk melindungi maklumat sensitif.

Cybersecurity Practices & Tools

- Melaksanakan amalan dan alatan *cybersecurity* yang teguh adalah penting untuk melindungi data perlindungan kesihatan daripada ancaman siber yang berkembang.
- Strategi utama, termasuk *password* yang kuat dan *two-factor authentication*, berfungsi sebagai barisan pertahanan pertama terhadap akses yang tidak dibenarkan.

Panduan Katalaluan (*password*) yang kuat

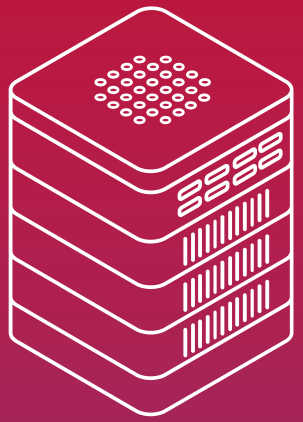
- Katalaluan yang kuat hendaklah mengandungi sekurang-kurangya 12 aksara, termasuk huruf besar, huruf kecil, nombor dan simbol khas.
- Elakkan menggunakan maklumat yang mudah diteka seperti tarikh lahir atau frasa biasa untuk meningkatkan keselamatan dan mengurangkan kerentanan terhadap serangan.

Two-Factor Authentication (2FA)

- *Two-Factor Authentication* (2FA) menambah lapisan perlindungan tambahan dengan memerlukan dua bentuk pengesahan yang berbeza sebelum memberikan akses.
- Ini dapat mengurangkan risiko akses tanpa kebenaran, walaupun katalaluan terjejas.

Penggunaan Perisian Antivirus

- Perisian antivirus dapat mengenal pasti dan meneutralkan ancaman persian hasa, memastikan sistem perlindungan kesihatan kekal dilindung daripada virus, trojan dan perisian tebusan (*ransomware*).
- Kemaskini dan imbasan yang kerap adalah penting untuk memastikan langkah keselamatan berkesan terhadap ancaman baharu dan berkembang.



Melaksanakan Firewall

- Firewall bertindak sebagai penghalang antara rangkaian dalaman yang dipercayai dan rangkaian luaran yang tidak dipercayai dengan mengawal trafik masuk dan keluar.
- Konfigurasi firewall yang betul adalah penting dalam menghalangi akses tanpa kebenaran sambil membenarkan komunikasi yang sah dalam perskitaran perlindungan kesihatan.

Tindak balas Terhadap Insiden Keselamatan Siber (*Cybersecurity*)

- Memahami tindak balas yang sesuai terhadap insiden keselamatan siber adalah penting untuk melindungi data perlindungan kesihatan dan meminimumkan gangguan operasi.

- Pendekatan berstruktur untuk tindak balas insiden memastikan tindakan pantas, mengurangkan kesan dan meningkatkan kesediaan untuk ancaman masa hadapan.

Langkah-Langkah yang perlu Diambil apabila Pelanggaran (*Breach*) Disyaki

- Mengasingkan sistem yang terjejas dengan serta-merta untuk mengelakkan kompromi data selanjutnya.
- Menilai tahap pelanggaran, mengenalpasti potensi kelemahan, memulakan penyiasatan awal.
- Menubuhkan pasukan tindak balas untuk menyelaraskan usaha pemulihan dengan berkesan.

Prosedur Pelaporan Insiden

- Semua pelanggaran yang disyaki mesti dilaporkan mengikut polisi jabatan dan keperluan kawal selia.
- Maklumkan kepada pihak-pihak berkepentingan utama (*key stakeholders*), termasuk pasukan seperti IT, undang-undang dan pematuhan, untuk memudahkan tindak balas diselaraskan dan pematuhan kepada Akta Perlindungan Data Peribadi (PDPA)

Pelan dan Strategi Pemulihan

- Mewujudkan pelan pemulihan komprehensif yang memperincikan tindakan langkah demi langkah untuk pemulihan data dan pemulihan sistem.
- Menguji dan mengemaskini pelan ini secara kerap untuk memastikan responsif terhadap ancaman baharu dan sejajar dengan amalan terbaik dalam keselamatan siber perlidungan kesihatan.

Program Latihan dan Kesedaran

- Melaksanakan program latihan berkala untuk semua kakitangan perlindungan kesihatan dalam mengenali dan bertindak balas terhadap ancaman keselamatan siber.
- Mewujudkan kempen kesedaran untuk menggalakkan amalan selamat, mengurangkan risiko insiden daripada kesilapan manusia.

Sekian,
Terima Kasih!

UNIT TEKNOLOGI MAKLUMAT, HOSPITAL KAJANG