Process Safety Beacon
Mesej untuk pekerja pembuatan
www.aiche.org/ccps/process-safety-beacon

An AIChE Technology Alliance
CCPS Center for Chemical Process Safety
aiche.org/ccps

Isu ini ditaja oleh
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Keselamatan Siber dan Operasi Kimia

Julai 2021

Rajah 1. Loji rawatan air Oldmar, Florida

Pada 5 Februari 2021, seorang pekerja di loji rawatan air di Oldsmar, Florida, menyedari bahawa kursor bergerak dengan aneh di skrin komputer kawalan, pada mulanya tidak ada kebimbangan; loji itu menggunakan perisian akses jarak jauh untuk membolehkan kakitangan berkongsi skrin dan menyelesaikan masalah IT. Penyelia juga sering mengakses komputer itu untuk memantau sistem fasiliti itu. Beberapa jam kemudian, operator itu melihat kursor bergerak dan klik kawalan loji itu. Dalam beberapa saat, penggodam itu mencuba untuk mengubah tahap natrium hidroksida didalam sistem dari 100 ppm menjadi 11,100 ppm. Operator itu dengan cepat mengesan perkara itu dan kembalikan natrium hidroksida ke tahap normal. Nasib baik, tiada kesan pada kualiti air.

Serangan *ransomware* pada Colonial Pipeline baru-baru ini menghentikan bekalan petrol ke pantai timur As selama beberapa hari.

Sistem syarikat anda mungkin bersambung dengan internet dan memerlukan perlidungan daripada ancaman siber. Terdapat banyak strategi yang digunakan oleh syarikat untuk mencegah ancaman siber seperti: *firewall*, perisian *anti-virus* dan polisi untuk melindungi dari *malware* dan virus komputer.

Lebih ramai orang bekerja dari jauh; ini telah meningkatkan peluang untuk serangan siber.

Adakah Anda Tahu?

- Penjenayah siber menggunakan perisian yang canggih untuk mengambil kesempatan terhadap pelbagai kelemahan untuk mencapai tujuan mereka.
- Serangan *ransomware* semakin meningkat dengan penjenayah menggunakannya sebagai alat menjana wang.
- Menurut satu kajian baru-baru ini, serangan siber berlaku setiap 39 saat. (Ref. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- *Phishing* ialah menghantar emel, kononnya dari syarikat terkenal, untuk mendorong individu untuk mendedahkan maklumat peribadi. Serangan ini adalah kaedah masuk utama untuk *malware*.
- Ancaman siber boleh memasuki sistem syarikat melalui emel, lampiran dan dari peranti storan mudah alih, seperti *thumb drives* atau peranti mudah alih yang lain.
- 95% pelanggaran keselamatan siber disebabkan oleh kesalahan manusia. (Ref. https://www.cybintsolutions.com/employee-education-reduces-risk/)

Apakah Yang Boleh Anda Lakukan?

- Sentiasa sahkan permintaan kemas kini perisian dengan IT sebelum meneruskannya, dan muatkan kemas kini yang diluluskan tepat pada masanya
- Pastikan *firewall* dan perisian rangkaian lain anda terkini dan dihidupkan.
- Pastikan untuk membuat salinan sistem dan data anda secara berkala.
- Gunakan kata laluan yang kuat untuk semua akses. Jangan berkongsi kata laluan atau akaun dan menukar kata laluan dengan kerap.
- Jangan simpan kata laluan pada pelayar web.
- Jangan klik pada pautan atau lampiran dalam emel yang dihantar daripada orang yang tidak anda kenali.
- Jangan sekali-kali memuat perisian yang tidak diluluskan pada mana-mana komputer syarikat; pastikan kunci akses dan peranti keselamatan fizikal yang lain dilindungi dengan betul.
- Sekiranya anda menggunakan akses jarak jauh, patuhi peraturan syarikat. Berhati-hati jika menggunakan laman internet awam.
- Sekiranya sesuatu di komputer anda kelihatan ganjil atau berbeza, minta bantuan! Ini mungkin penggodam yang cuba mendapatkan akses.

Serangan siber adalah benar. Anda adalah bahagian penting dalam pertahanan.