

Keamanan IoT adalah bidang teknologi yang terkait dengan pengamanan perangkat dan jaringan yang terhubung di internet of things ( IoT ). IoT melibatkan penambahan konektivitas internet ke sistem perangkat komputasi yang saling terkait, mesin mekanik dan digital, objek, hewan dan / atau manusia. Setiap " benda " disediakan pengidentifikasi unik dan kemampuan untuk mentransfer data secara otomatis melalui jaringan. Mengizinkan perangkat untuk terhubung ke internet membukanya hingga sejumlah kerentanan serius jika tidak terlindungi dengan baik.

**Tantangan keamanan IoT**

Sejumlah tantangan mencegah pengamanan perangkat IoT dan memastikan keamanan end-to-end dalam lingkungan IoT. Karena ide peralatan jaringan dan objek lain relatif baru, keamanan tidak selalu dianggap prioritas utama selama fase desain produk. Selain itu, karena IoT adalah pasar yang baru lahir, banyak perancang dan produsen produk lebih tertarik untuk memasarkan produk mereka dengan cepat, daripada mengambil langkah-langkah yang diperlukan untuk membangun keamanan sejak awal.

Masalah utama yang dikutip dengan keamanan IoT adalah penggunaan kata sandi hardcoded atau default , yang dapat menyebabkan pelanggaran keamanan. Bahkan jika kata sandi diubah, mereka seringkali tidak cukup kuat untuk mencegah infiltrasi.

Masalah umum lain yang dihadapi perangkat IoT adalah bahwa mereka seringkali terbatas sumber daya dan tidak mengandung sumber daya komputasi yang diperlukan untuk menerapkan keamanan yang kuat. Karena itu, banyak perangkat tidak atau tidak dapat menawarkan fitur keamanan tingkat lanjut. Misalnya, sensor yang memantau kelembaban atau suhu tidak dapat menangani enkripsi tingkat lanjut atau tindakan keamanan lainnya. Plus, karena banyak perangkat IoT "atur dan lupakan" - ditempatkan di lapangan atau pada mesin dan dibiarkan hingga akhir masa pakainya - mereka hampir tidak pernah menerima pembaruan atau tambalan keamanan. Dari sudut pandang produsen, membangun keamanan sejak awal bisa mahal, memperlambat pengembangan dan menyebabkan perangkat tidak berfungsi sebagaimana mestinya.

Menghubungkan aset lawas yang secara inheren tidak dirancang untuk konektivitas IoT adalah tantangan keamanan lain. Mengganti infrastruktur warisan dengan teknologi yang terhubung adalah penghalang biaya, sehingga banyak aset akan dilengkapi dengan sensor pintar. Namun, karena aset warisan yang kemungkinan belum diperbarui atau pernah memiliki keamanan terhadap ancaman modern, permukaan serangan diperluas.

Dalam hal pembaruan, banyak sistem hanya menyertakan dukungan untuk jangka waktu yang ditetapkan. Untuk warisan dan aset baru, keamanan dapat hilang jika dukungan tambahan tidak ditambahkan. Dan karena banyak perangkat IoT tetap berada di jaringan selama bertahun-tahun, menambah keamanan bisa menjadi tantangan.

Keamanan IoT juga terganggu oleh kurangnya standar yang diterima industri. Sementara banyak kerangka kerja keamanan IoT ada, tidak ada kerangka kerja tunggal yang disepakati. Perusahaan besar dan organisasi industri mungkin memiliki standar spesifik mereka sendiri, sementara segmen tertentu, seperti IoT industri, memiliki standar kepemilikan yang tidak sesuai dari para pemimpin industri. Berbagai standar ini membuat sulit untuk tidak hanya mengamankan sistem, tetapi juga memastikan interoperabilitas di antara mereka.

Konvergensi jaringan IT dan teknologi operasional (OT) telah menciptakan sejumlah tantangan bagi tim keamanan, terutama yang ditugaskan untuk melindungi sistem dan memastikan keamanan ujung-ke-ujung di area di luar bidang keahlian mereka. Kurva pembelajaran terlibat, dan tim IT dengan set keterampilan yang tepat harus ditugaskan untuk menjaga keamanan IoT.

**Pelanggaran keamanan IoT dan peretasan IoT**

Para pakar keamanan telah lama memperingatkan tentang potensi risiko sejumlah besar perangkat tidak aman yang terhubung ke internet sejak konsep IoT pertama kali berasal pada akhir 1990-an. Sejumlah serangan kemudian menjadi berita utama, mulai dari lemari es dan TV yang digunakan untuk mengirim spam ke peretas yang menyusup ke monitor bayi dan berbicara dengan anak-anak. Penting untuk dicatat bahwa banyak peretasan IoT tidak menargetkan perangkat itu sendiri, melainkan menggunakan perangkat IoT sebagai titik masuk ke jaringan yang lebih besar.

Pada 2010, misalnya, para peneliti mengungkapkan bahwa virus Stuxnet digunakan untuk secara fisik merusak sentrifugal Iran, dengan serangan dimulai pada 2006 tetapi serangan utama terjadi pada 2009. Sering dianggap sebagai salah satu contoh paling awal dari serangan IoT, Stuxnet menargetkan kontrol pengawasan dan sistem akuisisi data ( SCADA ) dalam sistem kontrol industri ( ICS ), menggunakan malware untuk menginfeksi instruksi yang dikirim oleh programmable logic controllers ( PLCs ).

Serangan pada jaringan industri terus berlanjut, dengan malware seperti CrashOverride / Industroyer, Triton dan VPNFilter yang menargetkan sistem OT dan industri IoT yang rentan.

Pada Desember 2013, seorang peneliti di perusahaan keamanan perusahaan Proofpoint Inc. menemukan botnet IoT pertama. Menurut peneliti, lebih dari 25% botnet terdiri dari perangkat selain komputer, termasuk smart TV, monitor bayi, dan peralatan rumah tangga.

Pada 2015, peneliti keamanan Charlie Miller dan Chris Valasek melakukan peretasan nirkabel pada sebuah Jeep, mengubah stasiun radio di pusat media mobil, menyalakan wiper kaca depan dan pendingin udara, dan menghentikan akselerator agar tidak berfungsi. Mereka mengatakan mereka juga bisa mematikan mesin, menginjak rem dan menonaktifkan rem sama sekali. Miller dan Valasek dapat menyusup ke jaringan mobil melalui sistem konektivitas di dalam kendaraan Chrysler, Uconnect.

Mirai, salah satu botnet IoT terbesar hingga saat ini, pertama kali menyerang situs web jurnalis Brian Krebs dan host web Prancis OVH pada September 2016; serangan mencatat di masing-masing 630 gigabit per detik (Gbps) dan 1,1 terabit per detik (Tbps). Bulan berikutnya, jaringan penyedia layanan sistem nama domain (DNS) Dyn ditargetkan, membuat sejumlah situs web, termasuk Amazon, Netflix, Twitter, dan The New York Times , tidak tersedia selama berjam-jam. Serangan menyusup ke jaringan melalui perangkat konsumen IoT, termasuk kamera IP dan router.

**Alat dan legislasi keamanan IoT**

Banyak kerangka kerja keamanan IoT ada, tetapi sampai saat ini tidak ada standar tunggal yang dapat diterima oleh industri. Namun, hanya mengadopsi kerangka kerja keamanan IoT dapat membantu; mereka menyediakan alat dan daftar periksa untuk membantu perusahaan membuat dan menggunakan perangkat IOT. Kerangka kerja tersebut telah dirilis oleh Asosiasi GSM, Yayasan Keamanan IoT, Konsorsium Internet Industri dan lainnya.

**Industri apa yang paling rentan terhadap ancaman keamanan IoT?**

Peretas keamanan IoT dapat terjadi di industri apa saja, dari rumah pintar hingga pabrik manufaktur hingga mobil yang terhubung. Tingkat keparahan dampak sangat tergantung pada sistem individu, data yang dikumpulkan dan / atau informasi yang dikandungnya.

Serangan yang melumpuhkan rem dari mobil yang terhubung, misalnya, atau pada alat kesehatan yang terhubung, seperti pompa insulin yang diretas untuk memberikan terlalu banyak obat kepada pasien, dapat mengancam jiwa. Demikian juga, serangan pada sistem pendingin obat perumahan yang dipantau oleh sistem IOT dapat merusak kelangsungan hidup obat jika suhu berfluktuasi. Demikian pula, serangan terhadap infrastruktur kritis - sumur minyak, jaringan energi atau pasokan air - bisa menjadi bencana.

Namun, serangan lain tidak dapat diremehkan. Misalnya, serangan terhadap kunci pintu pintar berpotensi memungkinkan pencuri memasuki rumah pintar. Atau, dalam skenario lain seperti peretasan Target 2013 atau pelanggaran keamanan lainnya, penyerang dapat menularkan malware melalui sistem yang terhubung - sistem HVAC dalam kasus Target - untuk mengikis informasi yang dapat diidentifikasi secara pribadi, menimbulkan kekacauan bagi mereka yang terkena dampak.

**Bagaimana melindungi sistem dan perangkat IoT**

Metode keamanan IoT bervariasi tergantung pada aplikasi IoT spesifik Anda dan tempat Anda di ekosistem IoT. Misalnya, pabrikan IoT - mulai dari pembuat produk hingga perusahaan semikonduktor - harus berkonsentrasi untuk membangun keamanan sejak awal, membuat perangkat keras anti-gangguan, membangun perangkat keras yang aman, memastikan peningkatan keamanan, menyediakan pembaruan / patch firmware dan melakukan pengujian dinamis. Fokus pengembang solusi harus pada pengembangan perangkat lunak yang aman dan integrasi yang aman. Bagi mereka yang menggunakan sistem IoT, keamanan perangkat keras dan otentikasi adalah langkah-langkah penting. Demikian juga, bagi operator, menjaga sistem tetap mutakhir, mengurangi malware, mengaudit, melindungi infrastruktur, dan menjaga kredensial adalah kuncinya.