行业要闻存档

Important Industry Information Index

http://www.isvoc.com/2016092218015.html

物联网安全缺乏是关键企业信息系统系统的巨大风险

22/09/16

NEWS ANALYSIS: The biggest single problem for security of the Internet of Things is that for the most part there isn't any and most of the things that need securing can't be readily updated to include it.

新闻分析：对物联网的安全最大的一个问题是，大多数没有任何和大多数的东西，需要确保

不能随时更新，包括它。

SARATOGA, Calif. —It's probably impossible to accurately state how many "things" comprise the internet of things (IoT) in enterprises around the world. Even best guesses are almost certainly wrong for the simple reason that until recently no one has even tried to count them.

萨拉托加 lif.

So let’s agree that the number is significant, so large that some estimates place the total IoT traffic on carrier networks may be more than half of all traffic.

因此，让我们同意的数量是显**着的**，**如此之大**，**一些估**计的地方，总的物联网流量的运营商网络可能超过一半的所有流量。

Contrary to some popular conceptions that the IoT is made up of internet-enabled refrigerators and toasters, in reality the most connected to the IoT are so mission critical that they may be more important to your business than the workstations that you probably spend far more time and effort to secure.

相反，**一些流行的概念**，**物**联网是由互联网功能的冰箱和烤箱，最现实的连接到物联网是关键任务，他们可能对你的生意更重要比工作站，你可能花更多的时间和精力来确保。

Depending on your business, they may be the numerical control machines in your manufacturing plant or perhaps even the automated forklifts that are being deployed in your warehouse. Or perhaps worse, the things that could be attacked might be the printers in your office. Or they might be something really big and scary—such as a nuclear power plant.

根据您的业务，他们可能是数控机床在制造厂或甚至自动叉车，被部署在你的仓库。或者更糟的是，可以攻击的东西可能是在你的办公室里的打印机。或者他们可能是真正的大和可怕的东西

I spoke about these possibilities with James McNiel, CMO of network management and security company NetScout. McNiel was a keynote speaker at the NetEvents global press and analyst summit here. He said that one of the major problems that’s currently below the security radar is ransomware being used not as a way to encrypt files, but instead as a way to prevent access to critical IoT devices.

我谈到这些可能性与 James McNiel，**首席**营销官 NetScout **公司的网**络管理与安全。McNiel **是一个主**讲人在 NetEvents **全球新**闻和分析师峰会在这里。他说，其中一个主要的问题就是目前低于安全雷达是勒索被使用的不作为方式对文件进行加密，而是作为一种方法来防止访问关键物联网设备。

“How much is it worth to a hospital to regain access to their blood gas analyzer so they can do surgery,” McNiel wondered.

并非所有的网站都是安全的，所以要确保您进行软件下载的来源网站是合法的可信的。

“这是值得医院重新访问他们的血气分析仪，他们可以做手术多少钱，”McNiel 想了想。

精电(00170)中期纯利 426 万元跌 98%不派中期息

Unfortunately, the potential cost to the enterprise by attacks on its devices is significant. McNiel reminded me that the Stuxnet attack by the United States and Israel against the Iranian nuclear efforts was ultimately and IoT attack. There, the Stuxnet worm drove the Iranian uranium centrifuges out of control while reporting normal operation to the operators.

不幸的是，潜在的成本对企业的攻击，其设备是显着的。需要提醒我，Stuxnet 攻击以色列和美国对伊朗核的努力最终与物联网攻击。在那里，Stuxnet 蠕虫将伊朗的铀离心机失控而报告正常运行操作。

While Stuxnet was effective in delaying the Iran’s nuclear program, the code escaped into the wild, where it’s available to anyone who wants to modify it as an attack against any type of device controller. There, the goal may not be to spin centrifuges out of control, but rather to implant software that sends a copy of all data handled by specific things to the party that launched the malware. Or it may be a ransomware attack that will make the thing unavailable until the ransom is paid.

而 Stuxnet 是延缓伊朗核计划的有效代码逃到野外，它提供给任何人谁想要修改它对任何类型的设备控制器的攻击。在那里，目标可能不旋转的离心机失控，而是植入软件，发送的所有数据处理的具体事情向党发起的恶意软件。或者它可能是一种勒索攻击，会使事情不可用，直到收到赎金。

The amount of damage that can be done to an organization is hard to estimate, but there are examples. McNiel suggested that malware sent to a printer, for example, could result in a copy of every document being printed being sent to a competitor or to a nation-state trying to steal intellectual property.

可以对一个组织所造成的损害的数量是很难估计的，但有例子。需要指出，恶意软件发送到打印机，例如，可能会导致一个副本每个正在打印的文件被发送到一个竞争对手或一个民族国家试图窃取知识产权。

Or it could be used to infect an automated forklift or inventory barcode reader to tell someone else everything that’s in your warehouse, which items move the fastest, when there are peaks in demand and even where the items are shipped.

或者它可以被用来感染一个自动化的叉车或库存条码阅读器告诉别人的一切，在你的仓库，

其中最快的项目移动，当有需求的高峰，甚至在那里的项目被运。

And that’s just scratching the surface.

这只是划伤表面。

The obvious question then is given that these devices are not secure and for the most part can’t be made secure, what do you do about it? For starters, when you buy new devices, specify that they must have some level of security, even if it’s just WPA2 encryption on WiFi.

明显的问题是，这些设备都是不安全的，因为大部分不能取得安全，你做了什么呢？首先，

当你购买新的设备，指定他们必须有一定的安全性，即使它只是 WPA2 加密的 WiFi。

The next thing you need to do is protect your existing devices so that it’s harder to break into them. McNiel suggests that this can be accomplished by protecting the network segments the devices connect to. He said that it’s also important to monitor them.

下一件你需要做的是保护你的现有的设备，让它更难进入他们。需要指出，这可以通过保护

网络段的设备连接完成。他说，监视他们也很重要。

“You need to look for anomalies,” McNiel said. He said that there are other means to protect your devices, including deception, so that a hacker or the malware that’s inserted on your network can’t tell whether it’s found the real device, or a simulation, such as a honey pot, which is a simulated device, frequently running on a server, that appears to be an inviting target, but instead is designed to trap the intruder or the malware.

“你需要寻找异常，”McNiel 说。他说，还有其他的手段来保护你的设备，包括欺骗，使黑客

或恶意软件的插入你的网络不能告诉是否找到了真正的装置，或模拟，如蜂蜜罐，这是一个

模拟装置，经常在一个服务器上运行，这似乎是一个诱人的目标，而是设计的陷阱或恶意入

侵者。

When you find anomalies, you then need to decide what’s causing it. But if it’s malware and it’s not preventing access to the device, then the next step is to monitor the device for exfiltration of data. If you find that, you can block the outgoing data and then examine the malware to see where it’s trying to transmit that data and what kind of data it want to send. With that information, you may be able to take further action such as blocking incoming connections from that site.

当你发现异常情况时，你需要决定是什么造成的。但如果是恶意软件并不是防止对设备的访

问，然后下一步是为数据外泄的监控设备。如果你发现，你可以阻止传出的数据，然后检查恶意软件，看看它试图传输的数据，它想发送什么样的数据。有了这些信息，您可能能够采取进一步的行动，如阻止来自该站点的传入连接。

But despite your best efforts, the bad guys will still get into your network. “You need to recognize when the device is legitimate and when it’s not,” McNiel said, adding that even with good security, your devices will be compromised. That means it’s always necessary to monitor those devices closely, so you can take corrective action before it spreads or gets worse, he said.

但尽管你尽了最大的努力，坏人还是会进入你的网络。”你需要认识到当设备是合法的，当它不是，”McNiel 说，补充说，即使有很好的安全性，您的设备将受到损害。这意味着它总是有必要密切监测这些设备，所以你可以采取纠正措施之前，它蔓延或变得更糟，他说。

信息安全很重要，如果没有强大的软件安全与保护技术，许多现代社会运作所依赖的基于软件的系统，如：电力、交通、通讯系统，医疗信息系统、数字版权管理系统、投票系统、财务系统等的核心部分，都将受到毁灭性的攻击。