Resistance, response and recovery

Nick Hawkins, Everbridge

In May 2017 the NHS was just one high-profile victim of the global ‘Wannacry’ ransomware attack. Patient data was exposed and compromised in the attack. In June of the same year, NotPetya, another crippling ransomware attack, targeted many of the EU’s largest companies. In the face of threats like this, how can you mitigate risk, limit the impact of an attack and expedite recovery? It comes down to the three R’s of cyber-security – resistance, response, recovery.

For companies and organisations today, it is not about whether you will be subject to a cyber-attack but when. The natural conclusion of accepting this premise is that managing a cyber-attack is no longer just about how well you are equipped to resist the attack in the first place but how you respond when your defences are broken and how quickly you recover to a normal state of business operation.

Hacking the backbone

During the Wannacry attack, hackers attacked the backbone of the NHS, tapping into computers, telephone lines, MRI scanners, blood-storage refrigerators and theatre equipment. Surgeons resorted to using their mobile phones to communicate with one another and critical information such as x-ray imaging was transported around the hospital on CDs.

The malware tapped into Windows XP. The NHS is becoming increasingly reliant on machines that are connected to the Internet and some reports suggest that 90% of NHS trusts run at least one Windows XP machine.¹

Firewall renewal dates for PCs will be logged. However, it is easy to forget when a portfolio of Internet-enabled devices needs to be updated for security. With the Internet of Things (IoT) expected to consist of millions of new connected devices in the future, this issue will become more critical.

Loopholes in security, combined with the fact that hackers are often one step ahead of defenders, makes a critical communications strategy extremely important. The cyber-defence industry may be remarkably quick to react – providing patches and closing down avenues of attack, but if communication with staff and customers is not clear and concise during and in the aftermath of a breach, serious reputational damage could ensue.

Resistance

This is not to say that resistance is futile. It isn’t – there are basic measures that every organisation should be taking to protect itself and make it harder for hackers to succeed.

“If communication with staff and customers is not clear and concise during and in the aftermath of a breach, serious reputational damage could ensue”

Keeping software and defence systems up to date is important. Critical information such as password resets, software updates and security best practices should be communicated with staff in a timely manner. This is where critical communications technology has an important role to play. Advanced platforms enable IT teams to send repeat reminders to staff en masse until they acknowledge receipt and respond confirming that password reset has taken place. Platforms that offer multi-modal enable messages to be sent via multiple delivery channels, which increases the likelihood of the desired action being carried out by staff.

Organisations should also consider how they protect and back up the data on their networks. Is the data encrypted and are you able to effectively roll back the clock to a time before the system was compromised?

The most efficient form of resistance is ensuring that your organisation is prepared should a cyber-attack take place. A practised response plan can significantly enhance your ability to recover. The plan should identify the various stakeholders that need to be communicated with, messaging templates and a system for escalation.

When a network is compromised, any communications across the network are potentially at risk. Suddenly, management cannot communicate effectively with employees without the risk that communications are being intercepted. Imagine trying to fix a compromised network without the ability to communicate with IT staff.

During the infamous hack of Sony Pictures, the company used a critical communications platform as an effective alternative to its compromised IT system.² It was independent of its own network and helped to keep employees informed and to cope with the immediate effects of the attack. Indeed, one of CEO Michael Lynton’s main takeaways from the incident was that he wished he had made it mandatory for every single Sony employee to be contactable on the system – most were, but others had to be signed up dur-
ing the attack. Preparing response plans prior to emergencies is often pushed down the to-do list: however, the benefits when an emergency strikes significantly outweigh the initial investment of time.

Response

The response plan created in the resistance stage will ensure that every staff member within the organisation knows exactly what steps they need to take in the event of an attack – even if it happens at four in the morning.

To effectively implement the response plan, communication is vital. When IT systems go down, an organisation needs to be able to communicate with its employees and co-ordinate an effective response. The longer this process takes, the bigger the impact. According to a study on how businesses respond to an emergency, carried out for the Business Continuity Institute, more than 80% of companies rely on internal email to communicate in a crisis. During a cyber-attack, it is likely that email will be compromised and should not be used, in order to avoid the attack spreading.

Cloud-based critical communications platforms are not reliant on one network, and operate entirely independently. This ensures that the bilateral lines of communication between management and staff remain open – even in the event of a cyber-attack or IT outage that may compromise an internal network, or a rush of calls that may overload a telecommunications network.

Response plan communications should address the following stages:

- **Assess**: What is happening? What is the impact? Determine the likelihood, severity, and impact of the incident.
- **Locate**: Who is in harm’s way? Who can help? Identify resolvers, impacted personnel and key stakeholders.
- **Act**: Which team members need to act? What do they need to do?
- **Analyze**: What have we done before? What worked? How can we improve communications?

Processes used for emergency communications. Source: BCI/Everbridge.

Departments responsible for an emergency communications plan. Source: BCI/Everbridge.
دریافت فوری
متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات