

Network Box advisory: 'Forgotten Security'

Part 3: Change Control

In the third of our advisory notices on 'forgotten security', we advise companies to implement a change control procedure prior to making any changes to their network security. The absence of a change control procedure can result in ad-hoc changes which risk compromising security.

In part two of our 'Forgotten Security' series, we investigated common errors in routing that lead to vulnerabilities in the network's security. In part one, we advised that companies should monitor their networks regularly for vulnerabilities as well as continue to defend the network against external threats, such as malware attacks. However, once you have discovered a vulnerability in the network, what is to be done to rectify this?

Some businesses rely on IT departments to spot the weak points in the system and rectify them as soon as possible. Whilst the need for a rapid resolution is understandable, this method exposes the company to another vulnerability – human error. A procedure should be in place, so that if and when a vulnerability is discovered, whoever makes the discovery knows exactly what needs to be done and when, and anybody needing to refer to what happened can find out who did what and when they did it. By implementing a change control procedure companies would automatically gain all these advantages.

What is change control?

Change control in this context is the formal process of controlling changes made to a system, network or application. It ensures that any changes introduced are done so in a co-ordinated, planned and thought-out way. If changes to a system are not controlled formally, or are not properly thought-through, they will often end up leading to network problems, or even reverse previously made system changes. Implementing proper change processes should result in minimal disruption and faster implementation time.

Why the lack of change control is a security concern

Mitigating Risk

Businesses that rely on one person to make changes to their networks, wrongly assume that the individual will not make a mistake. In fact they probably already have made them, and placed the organisation at risk. Having a change control solution in place would reduce this risk.

Increasing Complexity

Gateway defences are becoming more complex. Many applications penetrate the perimeter and you have remote users needing to access resources on the organisation's LAN. In a situation like this it is obvious that you don't make changes lightly or indeed frequently. If you are doing it

frequently then you either need a test network, or you are doing something wrong that is likely to increase the risk of compromise.

Implementation

In an ideal world, the team in charge of change control is separate from the team implementing the change (this is a good way of 'catching' any changes that might cause network problems). Alternatively, this could entail using a managed service company that would incorporate some of the change control function, or could be as simple as being a formal process you go through with a colleague not involved in the change.

The process should include the following basic steps:

1. Limit who is authorised to make changes to a system. The fewer people who can make changes, the lower the risk of error. Ensure that this policy is not broken, and that all requests for change go through an authorised administrator. Put in place limited user rights, so the system cannot be tampered with by unauthorised people. In larger companies, this could be done by using a ticketing system, which places a formal 'request' for the change, documenting it, and only allowing authorised (via password) team members to deal with the request. Involve two people if possible – often two people will come up with a more effective change plan than someone working in isolation.
2. Agree a set of change criteria: why do you need the change? What is the impact of it on the business? And what is the impact of implementing it? Often changes are made for no real business benefit, but with a great deal of disruption. For example, in the past, we discovered that an IT manager was dropping his company firewall late at night, so he could play games with friends over the Internet. Clearly not a business critical change! Document a set of criteria that must be met for any changes to be made, taking into account impact on the business, network downtime, cost and business need.
3. Assess the risk of making the change. This can be done through a formal risk assessment procedure (for larger companies), or by simply answering a set of questions that consider the impact of the change on other parts of the network or application, for example. Will the change have knock-on effects? Has it been tested? Include anyone who will be affected to ensure nothing is forgotten.
4. Record the change details as part of the formal change process. This is extremely important both in terms of identifying when and how the change was made, and also in case it needs to be reversed at a later date
5. Test the impact of the change on security. Often, we find that vulnerabilities in network security are caused not by malicious attacks, but by poorly-executed changes to the system that, for example, bypass security measures unintentionally.
6. Plan the change. Inform teams if there is likely to be any impact on productivity, or network availability.
7. Build and test the change - in a closed environment, if possible – to make sure the implementation has been done correctly.
8. Have a plan B. If the change doesn't work, or causes an unforeseen glitch, or has some other unexpected results, ensure it can be reversed, quickly (see point 4) to its previous,

safe configuration, while a review is done. In an uncontrolled environment it's not unusual for so many changes to have been made together that it becomes impossible to undo an error – which can be extremely costly to put right.

9. Implement the change. Timescales should have been agreed with all those involved (see point 6), and users briefed / trained as necessary on using the new system.
10. Review its success. Has the change been worth it? Has it had a positive impact on the business? Are individuals within the business using it in the correct way? It is important to review user implementation regularly and get feedback from them; this should influence future changes.

While formal processes can seem unnecessary or bureaucratic (particularly to smaller companies), they should, if used correctly, save both time and money, most notably spent on fixing the errors that are only too common in uncontrolled network changes.

For the latest security information and advice, visit www.network-box.co.uk, or read Simon Heron's blog at <http://blog.network-box.co.uk>. You can also follow Simon on Twitter at <http://www.twitter.com/networkbox>.

About Network Box:

[Network Box](#) Limited (NBL) is an international managed security services company, specialising in unified threat management (UTM). It continuously defends the networks of its customers using PUSH technology to instantaneously update protection, from 12 Security Operations Centres spread around the globe. NBL's customers in Asia, Australia, North America and Europe include companies such as BMW, Nintendo and Toyota, as well as banks, utilities companies and government organisations.