NEWS

NCSC issues fresh guidance following recent rise in supply chain cyber attacks

Guidance to help organisations assess the cyber security of their suppliers.

- New cyber security guidance issued in response to growing trend in supply chain attacks
- GCHQ's National Cyber Security Centre advises organisations to work with suppliers to identify weaknesses and boost resilience
- Businesses urged to take action as just over 1 in 10 review the risks posed by immediate suppliers

CYBER security experts have issued a fresh warning over the threat of supply chain attacks following a rise in the number of incidents.

The National Cyber Security Centre (NCSC) – a part of GCHQ – has today (Wednesday) published new guidance to help organisations effectively assess and gain confidence in the cyber security of their supply chains.

It follows a significant increase in cyber attacks resulting from vulnerabilities within supply chains in recent years, including some high-profile incidents such as the SolarWinds attack.

The new guidance is designed to help medium and larger organisations effectively assess the cyber risks of working with suppliers and gain assurance that mitigations are in place.

Supply chain attacks can cause far-reaching and costly disruption, yet the latest government data shows just over one in ten businesses review the risks posed by

their immediate suppliers (13%), and the proportion for the wider supply chain is just 7%.

Ian McCormack, NCSC Deputy Director for Government Cyber Resilience, said:

> "Supply chain attacks are a major cyber threat facing organisations and incidents can have a profound, long-lasting impact on businesses and customers.
>
> "With incidents on the rise, it is vital organisations work with their suppliers to identify supply chain risks and ensure appropriate security measures are in place.
>
> "Our new guidance will help organisations put this into practice so they can assess their supply chain's security and gain confidence that they are working with suppliers securely."

Cyber minister Julia Lopez, said:

> "UK organisations of all sizes are increasingly reliant on a range of IT services to run their business, so it's vital these technologies are secure.
>
> "I urge businesses to follow this expert guidance from our world-leading National Cyber Security Centre. It will help firms protect themselves and their customers from damaging cyber attacks by strengthening cyber security right across their supply chains."

The guidance has been published in conjunction with the Cross Market Operational Resilience Group (CMORG) which supports the improvement of the operational resilience of the financial sector, though the advice is for organisations in any sector.

It aims to help cyber security professionals, risk managers and procurement specialists put into practice the NCSC's 12 supply chain security principles and follows the government's response to a call for views last year which highlighted the need for further advice.

It describes typical supplier relationships and potential weaknesses that might expose their supply chain to attacks, defines the expected outcomes and sets out key steps that can help organisations assess their supply chain's security.

In addition to guidance focused on improving supply chain cyber resilience, the NCSC has published a range of advice to help organisations improve their own cyber security.

This includes the 10 Steps to Cyber Security guidance, aimed at larger organisations, and the Small Business Guide for smaller organisations.

PUBLISHED

12 October 2022

NEWS TYPE

General news

WRITTEN FOR

Small & medium sized organisations

Large organisations

Cyber security professionals

Public sector