Beat: News

Supply chain risk in cloud-based products

anti-virus (AV) software

London, 02.12.2017, 05:08 Time

USPA NEWS - NCSC CEO Ciaran Martin writes to permanent secretaries regarding the issue of supply chain risk in cloud-based products, including anti-virus (AV) software.

Russian antivirus companies: government and critically important national networks.

The issue of supply chain risk in cloud-based products, including anti-virus (AV) software, is receiving a lot of attention at the moment. For that reason the National Cyber Security Centre, a part of GCHQ, is today publishing specific guidance on managing the risk of cloud-enabled products. This guidance is applicable to every organisation in the UK and we will be promoting it within your departments and stakeholder organisations in the normal way. The reason for writing specifically to you is to address how departments should approach the issue of foreign ownership of AV suppliers. This is a complex and difficult area and we are seeking to explain it as clearly as possible "" a blog by our Technical Director, Ian Levy, sets out to do this.

The job of AV is to detect malware in a network and get rid of it. So to do its job properly, an AV product must (a) be highly intrusive within a network so it can find malware, and (b) be able to communicate back to the vendor so it knows what it is looking for and what needs to be done to defeat the infiltration. It is therefore obvious why this matters in terms of national security. We need to be vigilant to the risk that an AV product under the control of a hostile actor could extract sensitive data from that network, or indeed cause damage to the network itself.

That´s why the country of origin matters. It isn´t everything, and nor is it a simple matter of flags "" there are Western companies who have non-Western contributors to their supply chain, including from hostile states. But in the national security space there are some obvious risks around foreign ownership.

The specific country we are highlighting in this package of guidance is Russia. As the Prime Minister´s Guildhall speech set out, Russia is acting against the UK´s national interest in cyberspace. The NCSC advises that Russia is a highly capable cyber threat actor which uses cyber as a tool of statecraft. This includes espionage, disruption and influence operations. Russia has the intent to target UK central Government and the UK´s critical national infrastructure. However, the overwhelming majority of UK individuals and organisations are not being actively targeted by the Russian state, and are far more likely to be targeted by cyber criminals.

In drawing this guidance to your attention today, it is our aim to enable departments to make informed, risk-based decisions on your choice of AV provider. To that end, we advise that where it is assessed that access to the information by the Russian state would be a risk to national security, a Russia-based AV company should not be chosen. In practical terms, this means that for systems processing information classified SECRET and above, a Russia-based provider should never be used. This will also apply to some Official tier systems as well, for a small number of departments which deal extensively with national security and related matters of foreign policy, international negotiations, defence and other sensitive information. This is in line with the risk management posture adopted in the Government´s security classification system. Departments with responsibility for critical infrastructure may also want to discuss with us what implications this has for their sector where there may be national security concerns. The NCSC stands ready to advise departments in the normal way about how this can most effectively be implemented.

This is by no means the end of our work in this area and we will keep the issue under continuous review. We will provide further updates as necessary, both to central Government and other sectors, and to the UK as a whole, as required. This initial guidance is aimed only at central Government and we are not recommending action beyond central Government at this preliminary stage. That´s because our analysis of Russian state intent is that it targets national security interests. The vast majority of organisations and individuals are more likely to face cyber attack from criminals, against which AV products provide important protection.

As well as keeping this guidance under review, we are in discussions with Kaspersky Lab, by far the largest Russian player in the UK, about whether we can develop a framework that we and others can independently verify, which would give the Government assurance about the security of their involvement in the wider UK market. In particular we are seeking verifiable measures to prevent

the transfer of UK data to the Russian state. We will be transparent about the outcome of those discussions with Kaspersky Lab and we will adjust our guidance if necessary in the light of any conclusions.

Finally, it is worth reiterating, as Ian´s blog does, that the most important thing for departments to protect against threats in cyberspace is getting the basics right. Care in the selection of AV providers is just one part of an overall approach to managing risks to national security, but what will determine the success or otherwise of departments against the full range of cyber threats is keeping patching up to date, having good monitoring mechanisms, and all the other basics of good cyber hygiene we are promoting with your teams.

Your normal NCSC contacts will be able to help clarify any of these issues. This letter has been agreed with MI5, which is the responsible authority for investigating Russian espionage in the UK and is the NCSC´s key partner on protective security advice to Government.

Given the anticipated media interest in this subject, we are making this letter publicly available. Nonetheless I would be grateful if your team could actively promote awareness of it within the central Government security network and senior Government officials.

Ciaran Martin

CEO, National Cyber Security Centre

Article online:
https://www.uspa24.com/bericht-12520/supply-chain-risk-in-cloud-based-products.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement): Daren Frankish - GOV

Exemption from liability:
The publisher shall assume no liability for the accuracy or completeness of the published report and is merely providing space for the submission of and access to third-party content. Liability for the content of a report lies solely with the author of such report. Daren Frankish - GOV

Editorial program service of General News Agency:
UPA United Press Agency LTD
483 Green Lanes
UK, London N13NV 4BS
contact (at) unitedpressagency.com
Official Federal Reg. No. 7442619