Notice to Suppliers

Cyber Security information and recommendations

Originator: Neil Cassidy
Job Title: Director Cyber Security, Rolls-Royce plc
Business Unit: IT Risk & Compliance

NTS Number: 459
Issue: 1
Date: March 2019

For the attention of the Managing Director and the Head of IT or IT Security.

Dear Sir or Madam,

Scope/Applicability:

All Rolls-Royce plc suppliers.

Introduction:

Like many multi-national companies, Rolls-Royce can be a target for highly sophisticated cyber threats. We are also aware that our suppliers could be actively targeted, either to obtain access to information about our business or used as a means of gaining access to our network. We take this issue very seriously and closely monitor our security and systems.

This document is intended to remind you that you are a potential target for cyber threats and to share some information that may help you in identifying how your network could be targeted, whether that has in fact been the case, and what to do to reduce the risk. Much of this information is directed to cyber security activity that all companies should undertake and enforce, and you will no doubt already be undertaking much of this activity.

This information is designed for your IT or IT Security department and should be forwarded to them. Of course, your company remains solely responsible for implementing and monitoring security arrangements to fulfil its contractual and regulatory obligations. Whilst Rolls-Royce hopes that you will find this document useful, it is not intended to constitute advice on your company's IT security arrangements or to suggest that the implementation of the measures outlined will in itself be sufficient to ensure adequate levels of security.

What to look for:

We believe cyber attackers could attempt to use our suppliers to gain access to our networks. This would most likely be carried out through the exploitation of valid remote access connections through Virtual Desktop Infrastructure (VDI).

- In order to combat such an occurrence, we strongly recommend that suppliers: Ensure that all security tooling (AV, IDS, etc) is up-to-date and fully operational.
- Check anti-virus solutions for any potentially unwanted applications (PUA). In particular, look for any unexpected remote desktop support solutions such as VNC and Dameware.
- Monitor your estate for the unauthorised use of remote desktop support solutions. Endpoints with the ability to connect into the Rolls-Royce estate should be given special attention.
- Check for any unusual remote activity from the IP ranges 45[.]56[.]153[.]xxx and 64[.]64[.]108[.]xxx as we have intelligence that these are likely ranges that could be used.
- Ensure that logging is in place for all outbound connections from your estate into Rolls-Royce.
- Monitor for any unexpected account lockouts and ensure that Users report any unexpected activity on their endpoints (software unexpectedly starting or stopping, etc).
- Monitor for system log files being unexpectedly deleted.

- Check for outbound connections from your domain from devices that are not in your inventory – these may use a similar naming convention to your standard naming convention.
- Change user and administrator passwords on a regular basis and ensure that new, strong, passwords are enforced to avoid users simply incrementing an existing password (e.g. Password1 to Password2).

Conclusion:

As all companies are potential targets, working together to minimise the risk of cyber incursion is important. Threat actors are indiscriminate in their use of supply chains to access networks and therefore we would request that all our suppliers support us in preventing any malicious activity.

If you identify anything that causes you concern or suggests that anything untoward has occurred on your network, please immediately contact us on SOC@rolls-royce.com.

NTS Category:

General Information / Communication

Authorised by:

Neil Cassidy
Director Cyber Security, Rolls-Royce plc