#becrypt

Reducing Ransomware Risk

Beating crypto with crypto

The growth of ransomware has been driven by the devastating impact criminals can achieve by using cryptography to render an organisation's critical information and infrastructure inaccessible. If data is appropriately encrypted, and you don't have access to the encryption key, then for all practical purposes, you don't get access to your data. The nature of correctly implemented cryptography is typically this binary - unlike many of the tools used for cyber defence.

Most forms of cyber defence are, while often still necessary, regularly shown to be fallible: from traditional signature-based and AI-based technical measures, to people and process dependencies. Cryptography is different, based on mathematical proofs with highly predictable outcomes, and can therefore play a very important role in cyber defence for organisations that need to minimise risk and avoid many of the forms of malware compromise common today.

Technology developed in collaboration with the National Cyber Security Centre (NCSC) uses cryptography to validate the health and integrity of endpoint devices – typically the primary targets of ransomware. Cryptographically enforced device health measurements can be

used to determine whether or not endpoint devices are in a known good state, proving that none of the software executing or installed is either unauthorised or modified, and therefore verifying that the endpoint has not been compromised by malware to a level of certainty that non-cryptographic techniques cannot achieve.

Organisations within UK Government and the Critical National Infrastructure are increasingly using cryptographic device health measurements for their most sensitive assets, such as Privileged Access Workstations (PAWs), often as part of a shift to Zero Trust Architectures. However, for many organisations, the technology used for PAWs has broader relevance across the Enterprise, and can play a significant role in reducing ransomware related cyber risks.

Defence in **depth**

NCSC recommend adopting a 'defence-in-depth' approach to ransomware risk mitigation, with layers of defence that include both technical and procedural measures to provide different mitigations. Organisations should aim to increase the likelihood of detecting malware, while reducing its ability to spread and cause real harm. With the assumption that some malware will successfully infiltrate more vulnerable environments, or those subject to sustained targeted attack, steps should be taken to both limit the impact malware would cause, and speed up the response.

Making regular backups is a priority for ransomware protection, with careful consideration required for backup redundancy and offline storage. With the increased tendency for criminals to target backup systems before triggering ransomware, NCSC recommend the use of Privileged Access Workstations (PAWs), with multi-factor authentication for access to backup server administration. As outlined below, appropriately managed PAWs are not vulnerable to the types of attacks that most devices within an organisation are susceptible to. Preventing a criminal's ability to corrupt backups, significantly increases an organisation's resilience to ransomware.

Extending the **PAW** model

While PAWs can be an essential tool for securing administrative access, a recent trend within parts of the CNI, has seen PAWs deployed more widely across an organisation's user community, providing greater resilience not just for administrative activities, but for a wide range of business applications. This significantly reduces the risk of an initial malware infection occurring, and can simplify monitoring and response planning. PAWs are typically designed to consume applications and services via a secure browser, and as an increasing proportion of corporate services are delivered as virtualised or web applications, it has become increasingly viable for the widespread deployment of the same secure browser-based endpoints to support a far broader range of enterprise use cases, from remote working to DevSecOps and supply chain security.

The Paradox Secure Desktop platform was developed in collaboration with NCSC, and is an example of PAW technology now widely deployed across the UK Government and the CNI. Paradox provides a browser-based platform that can be configured to securely access a range of services, with rich support

for client applications including VPN and VDI clients.

Paradox mandates cryptographic health measurements of all software applications, drivers and operating system components, ensuring devices are in a known healthy state and free of malware before accessing corporate services. This removes a reliance on signature or anomaly detection for managed endpoint devices. According to NCSC guidance, combining robust device health measurements and device identity management with user identity management is core to the adoption of recommended Zero Trust Architectures, providing fine-grain control of access to protected services based on confidence of the integrity of endpoint devices.

Paradox implements a defence in depth architecture, preventing the launching of unauthorised or modified applications, as well as the prevention of privilege escalation which typically forms a necessary first step in ransomware infiltration. An integrated management platform automates patch and security management, with certificate-based device identity management complementing a range of user authentication options, for remote attestation to protected services.

Backup Checklist

NCSC highlight that up-to-date backups are the most effective way of recovering from a ransomware attack:

- Make regular backups of your most important files.
- Check that you know how to restore files from the backup.
- Regularly test that backups are working as expected.
- Ensure you create offline backups that are kept separate from your network and systems.
- Make multiple copies of files using different backup solutions and storage locations.
- Ensure your cloud service protects previous versions of the back-up from being immediately deleted.
- Ensure that backups are only connected to known clean devices before starting recovery.
- Scan backups for malware before you restore files.
- Regularly patch products used for backup.
- Backup accounts and solutions should be protected using Privileged Access Workstations (PAWs).
- Backup solutions should be protected using hardware firewalls to enforce IP allow listing.
- Multi-factor Authentication (MFA) should be enabled.

Balancing security, usability and cost of ownership

NCSC recommend that defence in depth architectures include the prevention of malware delivery using network-based services to control external website access, file ingress and content validation, coupled with endpoint security to prevent malware from running on devices through robust application control, health validation and automated vulnerability and patch management.

Paradox has been deployed within highly classified environments, due to its unique in-built health measurement functionality, but as an intuitive browser-based platform, Paradox is also widely used in less sensitive environments, such as dedicated endpoints for public access to online services, where its low cost of ownership and simplified management is as important as its robust security. For organisations making increased use of cloud and online services, Paradox allows the benefits of the secure browser-based desktop model to be extended through an organisation, providing a high level of resilience to ransomware and related attacks.

To find out more about how Paradox can support both privileged workstation and broader endpoint security contact info@becrypt.com.

About Becrypt

Becrypt is an agile London-based UK SME with 20 years cyber security expertise, established through the development and delivery of cloud, mobile and endpoint platforms. We supply governments and security-conscious commercial organisations, large and small, with a range of security solutions and services - from funded research, to commercially available products and flexible managed services. Becrypt have worked with UK Government and platform vendors to pioneer and deploy device health identity management products and services, based on the NCSC CloudClient Architecture.

https://www.becrypt.com/products/securedesktop/

Becrypt Ltd
Albion House
55 New Oxford Street
London WC1A 1BS
UK Company Number 4328430
Tel: 0845 838 2050

#becrypt