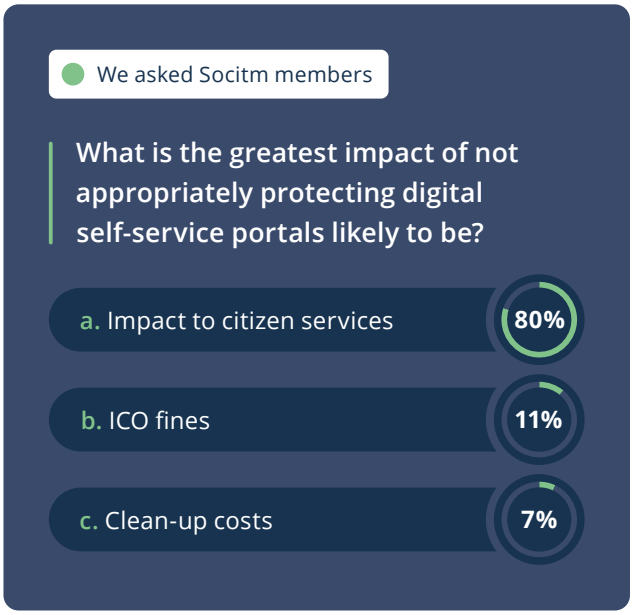
Helping Socitm members deliver seamless online public services

A virtual workshop

On 22 June 2020, Socitm and security software specialists Deep Secure co-hosted a virtual workshop on how to provide secure access for citizens to make service requests to online portals. Deep Secure account director, Paul Rutland, shares the key findings from the session and offers some leading practice recommendations.

Digital transformation is reshaping how we deliver public services, helping us engage dynamically with citizens, and transform standardized and manual public services to instantly personalised and automatic.

One of the most important steps we can take to support this transformation and to help ensure the availability of public services is to protect local authorities from malicious attacks and service disruption. If we fail to do this we risk a number of potential impacts, as the results of our workshop survey clearly show.



The majority of authorities in the UK now offer digital self-service portals in some form or another. This enables citizens to efficiently submit documentation such as images and forms to access public services including benefits, parking permits, disputes and reporting (potholes for example). The issue in handling data import in this way is the lack of assurance that the data is safe. Typically, the business process around the submission is direct access to an internal application or user desktop for review. This has caused many authorities to fail pen test audits and expose the authority to unnecessary risk.

It is widely understood that detection-based security software struggles to keep up with constantly emerging attacks concealed in documents and images.

We asked Socitm members

What percentage of attacks do you think detection-based security software can discover?

- a. 95-99% effective — 23%
- b. 85-94% effective — 38%
- c. 70-84% effective — 15%
- d. 50-70% effective — 11%

Attendees confirmed that a lack of trust in detection-based tools is a widely shared problem throughout local authorities. Based on this poll, it is believed that on average 1 in 10 attacks are potentially successful.

What is HMG's advice?

The UK's National Cyber Security Centre (NCSC) provides advice and support for UK plc – the public and private sector – in how to mitigate computer security threats. The key recommendations made can be found in the NCSC Guidance Pattern for the Safe Import of Data.[1]

The NCSC pattern provides a set of best practice recommendations based on Zero Trust. Following them can help the authority reduce IT operational costs (those costs associated with trying to identify false positives and negatives), reduce potential ICO impacts – by demonstrating conformance with the NCSC's guidelines and increase team productivity as less time and resource is spent on remediation, freeing up more time to be spent on digital transformation.

We asked Socitm members

What will be the potential impact of following the NCSC pattern?

- a. Reduce IT operational overheads — 11%
- b. Reduce ICO fines — 15%
- c. Ensure successful pen-tests/audits — 19%
- d. Enable more productivity — 7%
- e. All of the above — 46%

The conclusion is clear. Online portals are necessary for better citizen engagement but whether they are managed in-house or delivered by an outsourced IT service provider, they need to be appropriately protected, adopting the best practice recommendations of the NCSC pattern.

References

[1] Find out more about the NCSC's 'Pattern for Securely Importing Data': www.ncsc.gov.uk/guidance/pattern-safely-importing-data

More information

Watch a recording of the virtual workshop and get more information on the risks of public-facing portals and how best to mitigate them: www.deep-secure.com/videos/79-risk-of-public-portals.php

Read how Deep Secure helped a local authority safely import public data by following the NCSC's recommendations: bit.ly/2P2UH2I

Contact Paul Rutland for more information about protecting online self-service portals: paul.rutland@deep-secure.com

---

Socitm

Socitm is the society for innovation, technology and modernisation. Our vision is to be the preferred network for professionals who are shaping and delivering public services.

www.socitm.net

DEEP SECURE

Deep Secure's cloud-based Threat Removal solutions enable authorities to seamlessly integrate the NCSC recommendations for safely importing data, helping authorities deliver cost-effective seamless online public services.

www.deep-secure.com