Sweden's public sector must digitally transform to cope with post-pandemic challenges

As the COVID-19 pandemic took hold a year ago and governments implemented measures to try and contain the virus, a number of unexpected secondary consequences occurred. And Sweden was not immune – despite avoiding the most extreme restrictions, the Scandinavian nation implemented a number of restrictions too.

Arguably at the forefront of these consequences was a shift in working and living patterns as a result of national lockdowns – including a seismic move to working from home. Among the many difficulties and complexities that this brought, one of the most significant was a dramatic rise in cyberattacks. Work from home policies exposed all and any vulnerabilities and weaknesses in organisations' security networks. For organisations in the public sector, including emergency services, public transport, infrastructure and education sectors, this threat is particularly critical: if their data and systems are compromised, chaos and potential breakdown of an already pressured society may well ensue.

What's more, this increased pressure on networks may lead to multiple points of failure in organisations' technology stacks – increasing outages, as well as the possibility of public dissatisfaction. For most sectors, outages may result in dramatic amounts of lost revenue and reputational damage. For public sector businesses, as with cyberthreats, an outage will likely have even broader, deeper and more significant consequences.

And the public sector has arguably been under greater strain than most during and as a direct result of the pandemic. With hospitals overrun, public transport systems underused, organisations in this sector simply cannot afford the cost or reputational damage associated with cyberattacks and outages.

But these changes are no longer just a minor inconvenience that companies will have to endure in the short term before reverting to normal. After over a year of a new way of living, many of these changes are largely irreversible. After seeing that working from home is possible, many will demand the flexibility and choice to continue to do so once COVID-19 is behind us.

In light of this, then, and in order to avoid losing their best employees to competitors who offer this flexibility, companies must find a way to mitigate changing patterns of consumption and cyberattacks while facilitating a sustainable, secure way for their employees to work from home, if they so choose.

But with cyberattacks seemingly exponentially growing in scale and sophistication, even the largest and most established businesses are not immune. So how can such organisations effectively manage their exposure to cyberthreats?

A growing cyberthreat landscape

As the world saw a mass exodus from centralised working environments to the vast majority of people working from home – and not just office workers: everyone from educators to GPs to IT providers. Among the plethora of complications this has caused for businesses, at the forefront has to be the dramatic increase in cybersecurity threats. In fact, our research shows that hacking attempts increased by over 300% in the last 12 months.

Sweden is no exception. In October last year, Gothenburg-based security company Gunnebo, which specialises in enhanced security for buildings, was the victim of a cyber-attack which resulted in 38,000 files being leaked – including blueprints of bank vaults, monitoring and alarm equipment, and security functions for ATMs. Other sensitive documents leaked included information from the Riksdag (Sweden's national legislature and the supreme decision-making body) and classified drawings of the Swedish Tax Agency's office in Solna.

And two months later, it was revealed that dozens of Sweden's top businesses, including the Swedish Space Company, were targeted in what was described as the largest cyberattack in the country's history.

It is no coincidence that this rise in cybercrime occurred in parallel with the pandemic. As working from home proliferated, cyber-attackers seized the opportunity to exploit the vulnerability of remote workers. Without the security protections of office systems, with no warning or gradual adjustment period, their compromised IT systems and security networks, and compounded by an increased reliance on technology for day-to-day communication that would have previously happened in person, they were the perfect target for such attacks. And, scarily, research shows that 47% of individuals fall for a phishing scam when working from home.[1]

What's more, many firms in the public sector, for instance, often employ a 'Bring Your Own Device' (BYOD) approach, in contrast to a 'Corporate Owned Personally Enabled' (COPE) approach – particularly as the shift to work from home happened so suddenly with little time for companies to adequately prepare. Because employees can use their personal devices (phones, tablets, or laptops) to access corporate information, the risk of cyberattacks is exacerbated further for such businesses – who can least afford the cost of cyberattacks.

Mitigating the threat

In response to the cyberattacks, Sweden announced in February this year that it plans to establish a national cybersecurity centre, making it the latest Nordic country to bolster its cyber defence ambitions and capabilities in the face of the growing cyberthreat landscape.

This is certainly a step in the right direction – but it is companies, whose own profit margins are on the line as a result of such attacks, that must take control of their own destinies.

It is understandable that, following the economic consequences of the pandemic, firms across industries are desperately trying to protect their profit margins and cut costs wherever immediate returns aren't guaranteed – particularly in the public sector, where budgets are already stretched. For many, then, that meant postponing – and even cutting – budgets for departments that, in the current landscape, need it the most. IT security, cybercrime, and fraud department budgets in the financial services sector, for instance, have been cut by almost a third in the past 12 months[2]– meaning that departments have fewer resources to fight a greater threat.

With the cost of a data breach resulting from remote working averaging $137,000, according to Deloitte[3], it is critical that businesses spot an attack before it has major consequences.

Comprehensive monitoring and alerting tools are essential for safeguarding the health of IT networks and infrastructures. Solutions like ITRS's OP5 Monitor enable early problem detection, and notify you when your infrastructure is not working as expected.

And this can be further enhanced by ITRS's Log Analytics add-on. Built upon the best machine learning libraries that can identify trends and predict behaviour of the systems in your infrastructure, the neutral networks help to detect real-time anomalies – including non-standard network traffic that might suggest hacking attempts. More, by providing a fully transparent overview of logs, the tool allows users to monitor, in real time, everyone who logs into the application, runs queries, exports the data, or changes user permissions.

Increased pressure, increased outages

Over the last twelve months, systems have faced significantly increased pressure as a result of not only changing working patterns, but also shifting consumer demands; McKinsey observed that we have covered a "decade in days" in terms of digital adoption as a result of COVID-19.[4]

As a result, not only is the likelihood of outages greater as online traffic has drastically risen, but the tolerance for such outages is decreasing – particularly for services deemed essential.

In light of this, it is more important than ever for public services companies to put themselves in the shoes of the end user in order to ensure they are operationally resilient in the face of these challenges. This is called synthetic monitoring, and it provides the most fundamental test of IT availability: whether a customer can gain access.

Tools like ITRS's Synthetic Monitoring provides organisations with this ability by giving organisations visibility into the performance and availability of their most critical systems – including websites, applications and APIs. In addition, it also simulates a realistic user experience across all services from 180+ locations across 60+ countries worldwide, giving firms rapid insight into where things are very slow or – in the worst case – unavailable.

By understanding exactly how their customer is experiencing services 24/7, business leaders and IT teams don't have to wait to hear about outages and systems failures from their clients. Synthetic monitoring ensures an optimal user experience 24/7, even – and, indeed, especially – when demand is at its highest.

Benefits of Cloud

In the face of increased pressure on both ensuring continuity, and on companies' bottoms lines – and this is arguably truer for the public sector than any other – optimisation is key. For companies that have their own data centres and maintain their own IT infrastructure, moving to the Cloud can increase their agility and ability to respond to consumer demand, as well as making it easier to control costs.

However, for those who fail to optimise their Cloud costs, they may see their costs soar, rather than decrease. And on average, businesses that use the Cloud are wasting 30% of their cloud spend – which is an ongoing inefficiency, given that public Cloud charges by the hour.

One of the main causes of this is the use of the 'like for like' or 'lift and shift' approach, which see businesses counting their virtual machines and then mapping them to their chosen Cloud provider. This can result in the existing inefficiencies in their onsite IT estate being replicated in the Cloud. And the extra costs are multiplied, because, while in the physical data centre, the company already owns its servers – regardless of whether they're being used at full capacity – while in the public Cloud, they will be paying for the entire capacity every single hour. While it is true that capacity needs to be in place for demand surges, a business can make significant savings on their excess Cloud capacity with the right tools. In addition, because the Cloud is scalable, businesses do not need to pay for 'just in case' capacity.

However, when used correctly, the Cloud can deliver scalability and flexibility as well as lowering IT spend. As such, it is crucial that organisations have the right tools and understanding to best align Cloud spend with Cloud usage. In reality, many companies are still in a hybrid environment, with some of their IT estate on site and a lot of their new IT, such as greenfield apps, moved to the Cloud, suggesting phased momentum in their Digital Transformation.

Meanwhile, IT estates are growing ever bigger and more complex. Despite the business shift towards digital, many still think along physical lines. For example, ITRS's head office is in London while in reality the bulk of the business is taking place off-site in the Cloud.

There's no question about it: the COVID-19 pandemic has changed lives – and working patterns – forever. And while investing in measures like monitoring tools can seem an unnecessary, irritating expense at a time of intense cost and profitability pressures, particularly for smaller businesses, they are in fact the ones who need it the most, without the resources to be able to pay the price of a potential attack or outage.

Bibliography

[1] https://www.tessian.com/blog/why-we-click-on-phishing-scams/#:~:text=In%20a%20recent%20survey%20conducted,a%20phishing%20email%20at%20work

[2] https://markets.ft.com/data/announce/detail?dockey=600-202104280300BIZWIRE_USPRX____BW5365-1

[3] https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

[4] https://www.mckinsey.com/~/media/mckinsey/industries/retail/our%20insights/how%20covid%2019%20is%20changing%20consumer%20behavior%20now%20and%20forever/how-covid-19-is-changing-consumer-behaviornow-and-forever.pdf