CIONET What's next. | Hitachi Vantara

RANSOMWARE RECOVERY: BE PREPARED, NOT SCARED

EXPLORING FIRST-HAND EXPERIENCE, RISK MITIGATION, AND BEST PRACTICE

Discussion Documents

November 23

Ransomware Recovery: Be Prepared, Not Scared

Exploring first-hand experience, risk mitigation, and best practice

Ransomware Recovery: Be Prepared, Not Scared' – a CIONET executive dinner in association with Hitachi Vantara – took place on 9 November 2023 at the Hotel Villa Dagmar, Stockholm.

In a world where cyber and ransomware attacks are at an all-time high and proving increasingly sophisticated, it's becoming ever more apparent that it's a matter of not if but when your organisation faces such a threat.

Last year alone there were over

490 million

ransomware attacks worldwide.

When threat turns into a full-scale attack, do you know what to do? How sophisticated – and up-to-date – are your mitigation plans? And, in particular, do you know how long it will take you to recover one of your most valuable assets – your data? Hours? Days? Weeks? Months?

It is the threat of ransomware and what to do about it that formed the basis of a specially-arranged CIONET executive dinner hosted in Stockholm in early November. 'Ransomware Recovery: Be Prepared, Not Scared' was organised in association with Hitachi Vantara and attended by senior security professionals from a range of Swedish organisations.

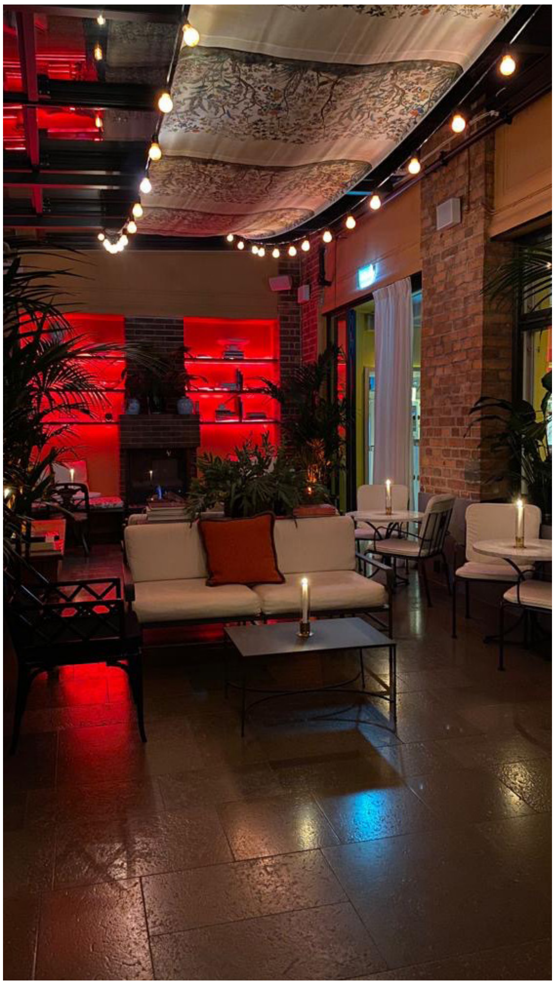
The cost of an attack

Providing opening remarks on behalf of Hitachi Vantara, Senior Solution Architect Anders Lindquist observed:

> *"Our dependency on IT systems just keeps growing and that makes us increasingly vulnerable."*

As such, he said, ransomware recovery has become a natural part of business continuity planning.

Lindquist pointed out that the average ransomware pay-out is an estimated $1.5 million, a figure that doesn't take account of the "clean up" costs, the loss of business, and the quantifiable reputational damage. Recovery times are going up, too. Accordingly the average interruption time is 24 days, compared to 15 days three years ago.



Talk of ransomware pay-outs led naturally to another question: should organisations pay to get their data back? By a show of hands, the vast majority of attendees indicated that they would not pay. Why not? Beyond the ethical dilemma of rewarding criminal intent, there are practical implications as well.

> *"Even if you pay, there's no guarantee you'll get the data back anyway."*

When it was suggested that organisations might say one thing in public but would act differently in private, some accepted this to be the case. Payments are made. Another delegate pointed out that those average pay-out numbers should themselves be taken with a pinch of salt given it is in the cyber criminals' interests to inflate the effectiveness of their work.

Continuous training and other best practices

Turning to best practice, mitigation planning and continuous training were cited as key elements in any effective prevention and recovery strategy. Continuous training means more than obliging staff to read the latest set of instructions. Users need to be tested. One well-known cloud provider, for example, insists on monthly tests. Speaking of tests, phishing exercises remain a popular way of keeping teams on their toes.

> *"The same people fall for it every time,"*
> noted one attendee.

Another often missed consequence of a successful ransomware attack is the impact it can have on the teams charged with recovery. Stress and long hours that follow an attack require a direct intervention, insisted one attendee. A behavioural psychologist may be an unexpected but vital member of the team in future.

Cyber security as a team sport?

One attendee posed a question that resonated with fellow security professionals: "Who owns the problem?" There is an overwhelming assumption in many organisations that IT owns the security problem. However, as different business departments wield greater autonomy when it comes to the adoption of technologies – notably software as a service (SaaS) – so those department heads need to take greater accountability when things go wrong. This is security as a team sport and it requires a culture shift.

More broadly, most attendees said their organisation was getting better at sharing experiences and best practices with others within their vertical market. Inevitably, that means opening up to direct rivals. It's worth it, however, because intelligence sharing is central to tackling a problem that afflicts all parts of the economy. In one sector, a Signal social sharing group has been set up for this very purpose – alerting others within the market to an ongoing threat and, subsequently, to share learnings post event.

So are we better at combatting ransomware than we were five or ten years ago?

"We are better," said one attendee.

"Unfortunately, the other side has also got better."

Ransomware Rec
Be prepared, not sca
Thursday 9th November 2023, Villa Dagmar, Stock
CIONET
Hitachi Vantara
hank you very much for spending your eveni
forward to seeing you again

CIONET
What's next.