Secura

A BUREAU VERITAS COMPANY

CYBERSECURITY IN RETAIL

BEST PRACTICES

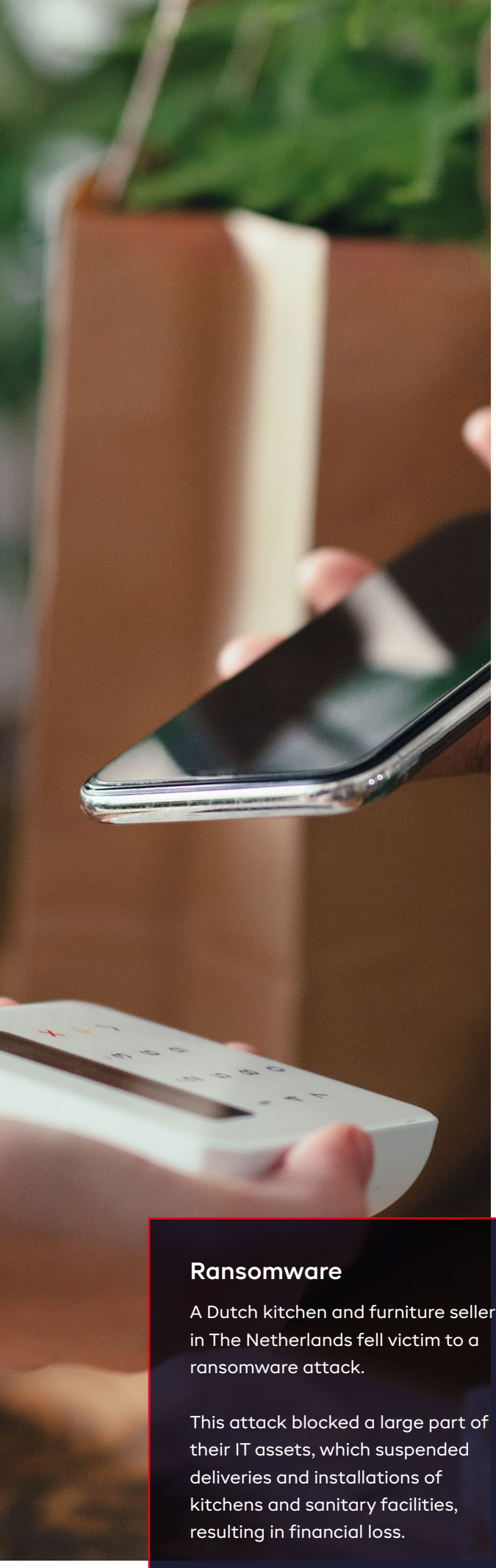
November 2021

Cybersecurity in Retail
Best Practices

During the coronavirus pandemic many retailers had to close their physical shops and increase online sales and move to working remotely. Rapidly they had to adapt their channel mix and transform quickly to embrace new digital ways to offer and deliver to their clients. E-commerce websites and applications were developed under high pressure with a user-friendly experience in mind, often bypassing typical cybersecurity processes. This speedy transition created a window of opportunity for cyber criminals and as a result, many retail organizations were hit by ransomware.

According to the Retail Platform Netherlands the damage due to cyber attacks in The Netherlands is estimated at 10 billion euro[1]. Many organizations have not assessed the security posture of their new IT landscape yet as many have been struggling to cope with all the changes. However, with the increasing number of cybersecurity attacks, the investment in cybersecurity safeguards and resilience cannot be delayed further. In this whitepaper we share some commonly seen risks and attacks specific for this sector, taken from our experience in supporting this sector. After discussing these specific risks we will provide some general best practices to consider.

[1] https://www.retailplatformnederland.nl/cyber-security/



Ransomware

A Dutch kitchen and furniture seller in The Netherlands fell victim to a ransomware attack.

This attack blocked a large part of their IT assets, which suspended deliveries and installations of kitchens and sanitary facilities, resulting in financial loss.

Common Risks and First Steps to Take

Secura performs security assessments for a large selection of retail organization from supermarkets to high-end niche retailers and complete e-commerce platforms. We assess these clients from a people, process and technology perspective. Secura recommends that you include at least all of these risks in your risk assessment.

Ransomware – Are Your Procedures and Processes Ready?

The ransomware business model has proven to be very effective and continues to be the main threat to the retail sector[2]. The financial toll for rectifying a ransomware attack can be substantial; when you considering downtime which results in lost sales and labor costs. This is next to the ransom sum, which, although ill-advised, may sometimes be the unfortunate final option and might not even result in a decrypt.

For retail organizations, it is essential to assess ransomware readiness, which includes amongst others the following points:

- Do you have an overview of key systems to support your first line of sales and support your key channels?
- Do you have off-line back-ups in place, what is your back-up policy and did you test restoring systems in a Business Continuity Test?
- Is the restore time reasonable and appropriate for your risk appetite?
- Do your back-up or fall-back systems also include vendor supplied systems?
- Did you perform a table-top exercise to practice your response to commonly known ransomware attacks on your systems? What systems are affected and how do you recover?
- Keep in mind: cloud solutions are not immune to ransomware attacks and cloud backups can be deleted by criminals.

[2] https://partnernews.sophos.com/en-us/2021/08/resources/the-state-of-ransomware-in-retail-2021/

Secura
A BUREAU VERITAS COMPANY

Data Theft From Key Systems – Are Your Systems Protected?

The attack surface of a typical retail organization grows over time, and is an attractive target for cyberattacks. Due to the nature of the business, retailers often have a distributed IT environment with connected point-of-sales (POS) devices, which also hold financial and personal customer data. As retailers are highly dependent on brand reputation and hold personally identifiable information (PII), an attack impacts brand reputation directly while possibly leading to fines from regulators. To monetize their breach attackers can auction the customers' data, including payment information, in the black market or use the threat of disclosure to increase the chances of a payment.

Concerning the security of your data, you should consider the following points:

- Have you performed your (mandatory) DPIAs?
- Do you have simple playbooks ready and know how to communicate a breach to customers and regulators?
- Do you have a retainer with a digital forensics and incident response provider?

Supply Chain Attack

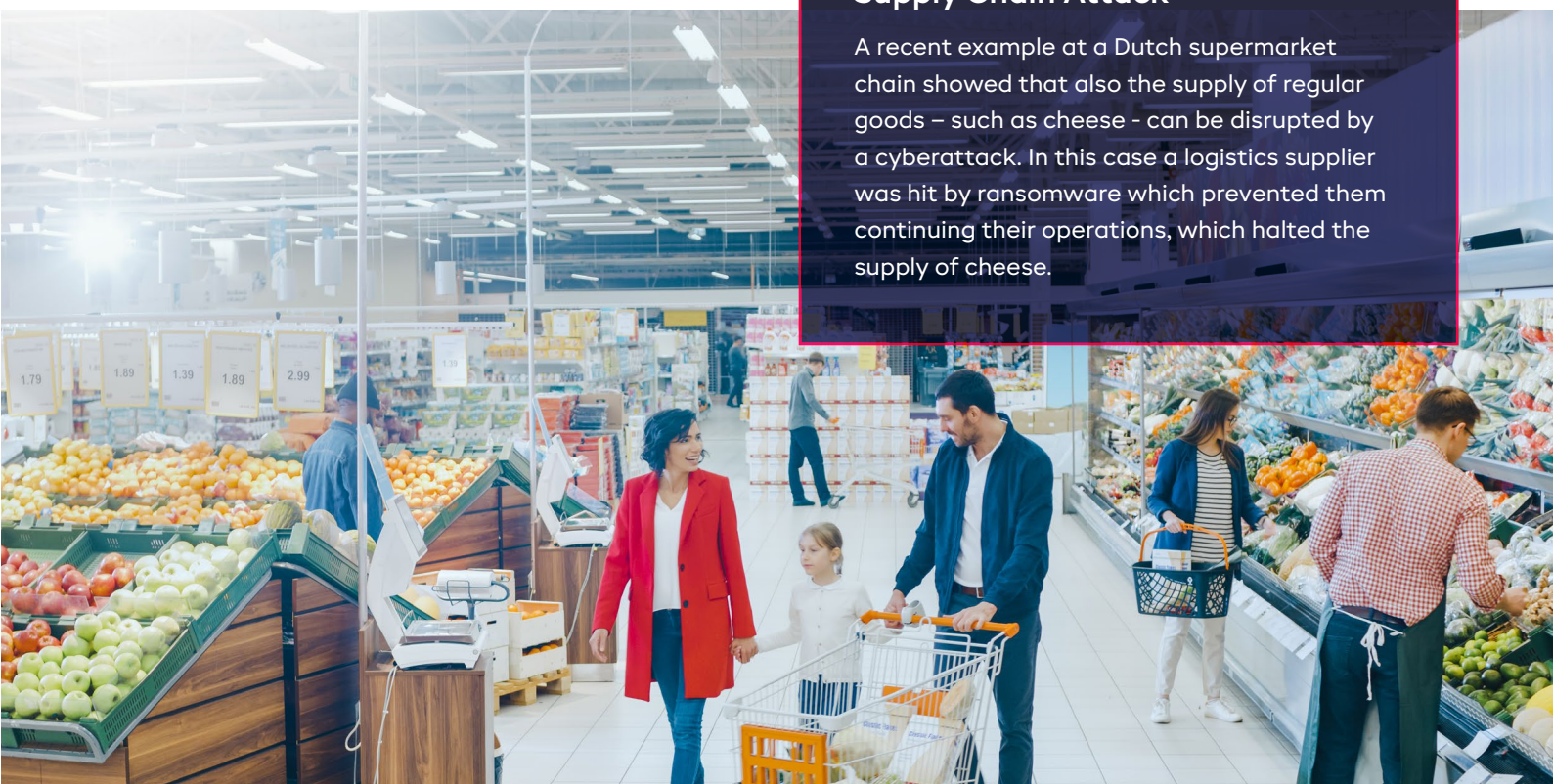
A direct cyberattack can have a disastrous effect on the operation. However, many retailers are also dependent on suppliers for their operation and these supply chains remain vulnerable. Typically, supply chains consist of a network of vendors that support the retailer's business. Although your retail organization is fully compliant and secure, a vulnerable supplier might impact your retail business.

To guarantee the continuity of your supply chain, it is wise to check the following points:

- Do you know which suppliers play a critical role in your core processes?
- Do your SLAs contain concrete and actionable security requirements or a right to audit?
- Does you procurement process include setting security requirements for new vendor selection? Does this go further than just asking for an ISAE3402?
- Do vendors inform you of breaches or vulnerabilities in their products? How does this work in practice?

Supply Chain Attack

A recent example at a Dutch supermarket chain showed that also the supply of regular goods – such as cheese - can be disrupted by a cyberattack. In this case a logistics supplier was hit by ransomware which prevented them continuing their operations, which halted the supply of cheese.



Network Segregration

During a recent assessment Secura conducted, it was found that the publically and physically accessible network connections of devices (fridges, scales) at a retailer's shop location allowed direct access to the internal network.

IoT – Have You Taken The Rights Steps To Minimize Risk?

The number internet-of-things (IoT) devices connected to the internet is increasing rapidly. These devices, ranging from printers to point-of-sales hardware, typically have limited security controls built-in and might be outside the asset management inventory (shadow IT), and often lack security updates or certification. In the dynamic environment of the IoT domain, a security threat could be your attacker using the kids' digital play wall as an entry point to get onto your network by example.

To check your IoT-devices, we advise to check the following points:

- Is the default configuration reviewed for security issues (such as default passwords and reachable services)?
- Do you have an overview of the IoT devices connected to your network or the internet? Can attackers reach these devices from the internet?
- Is the firmware of the IoT devices up-to-date and reviewed periodically?
- Can you remotely update access the devices? Can your vendor remotely access them?
- Are the devices on the same core IT network or are they on a different network with a different security level?

Cloud – Is Your Environment Configured Appropriately?

Finally, the general trend to move assets to the cloud is also present within the retail sector. There are many benefits to using cloud computing technologies, but this technology also poses new risks and security challenges. The cloud solution needs to be managed and configured properly.

We advise to check the following points related to the cloud:

- Do you train your cloud engineers on security topics? (standard courses are available)
- Have you conducted a configuration security review of your cloud environment?
- Have you enabled multi-factor authorization for accounts with privileges within your cloud environment?
- Do you have a conditional access policy defined?
- Do you know when someone changes your cloud resources? (Logging/monitoring)
- Do you apply the principle of least privilege?

Getting To The Next Level

A clear security strategy and clear risk management is needed to guide risk-based security approach. Many retailers have to address the deferred risks and vulnerabilities that were introduced in the transformation during the COVID-19 crisis. To address this and the ever-growing challenges in protecting your information assets safely, a holistic information security strategy is therefore essential. This strategy sets the goals and direction for the information security program and includes the objectives and desired state of the information security posture. Cyber risk management is crucial in an optimal balance between cost and minimizing vulnerabilities in a secure operation. Starting with a basic asset inventory, performing an annual risk analysis and taking actions upon this analysis is a great first step. Guidelines like ISO 27001 provide a framework that you can adopt, even without going through the formal certification.

Generally, we see that third-party vendor management is an underrated component of a mature cybersecurity strategy. The supply chain attacks of the recent years show, and the Sunburst attack in particular, how quickly an attack on a third-party can affect your operation. For retailers with substantial third-party dependence, it is worthwhile to create third-party use cases in the security operating center (if applicable), applying zero-trust policies, creating playbooks for third-party supply-chain attacks and mandate security training and SLAs in third-party contracts.

Thirdly, we see especially larger retailers investing more and more in security behavior change, by ensuring their employees are educated. This enables them to have a security mindset, which supports efficiency in updating basic security requirements, security developments, security processes and company policies. Hence staff starts to make better decisions bottom-up and thereby preventing risks and decreasing fraud. This ranges from training developers on security programming to helpdesk staff on clicking certain malware leading to a ransomware attack. Behavior and ingenuity of your employees is essential to uncover security gaps and your employees are therefore the strongest link in securing your business.

Lastly, Secura recommends a 'respond/recover' security strategy. An organization should not only prevent a cyberattack but be ready in the case of an event. This means that when a security incident occurs, actions taken should be intended to mitigate the impact as much as possible. Detect incidents quickly, diagnose accurately and determine root causes, contain and minimize the damage, restore the operation, improve and document the incident. Make sure to test your incident response processes during simulations – such as ransomware simulations – to verify the procedures and actions taken when a security incident occurs. In today's world it is no longer a question of 'if' an attack will happen, but 'when'.

How Can Secura Help?

Secura is an independent cybersecurity expert, providing insight into your security. We take a holistic approach from a people, process and technology perspective and have experience with many different technologies and markets. Secura security consultants can help in defining the information security program and settings clear security objectives for your organization by conducting risk and security assessments.

Join The Discussion!

Join our industry roundtables! Share lessons learned and ask any questions you might have on increasing your overall cyber resilience or for instance more specifically about your ransomware readiness!

Register here:
https://www.secura.com/retailroundtable

Secura
A BUREAU VERITAS COMPANY

BUREAU VERITAS
Shaping a World of Trust

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

Vestdijk 59
5611 CA Eindhoven
Netherlands

T +31 (0)88 888 3100
E info@secura.com
W secura.com

Follow us on