TRUESEC

Fortifying the Future

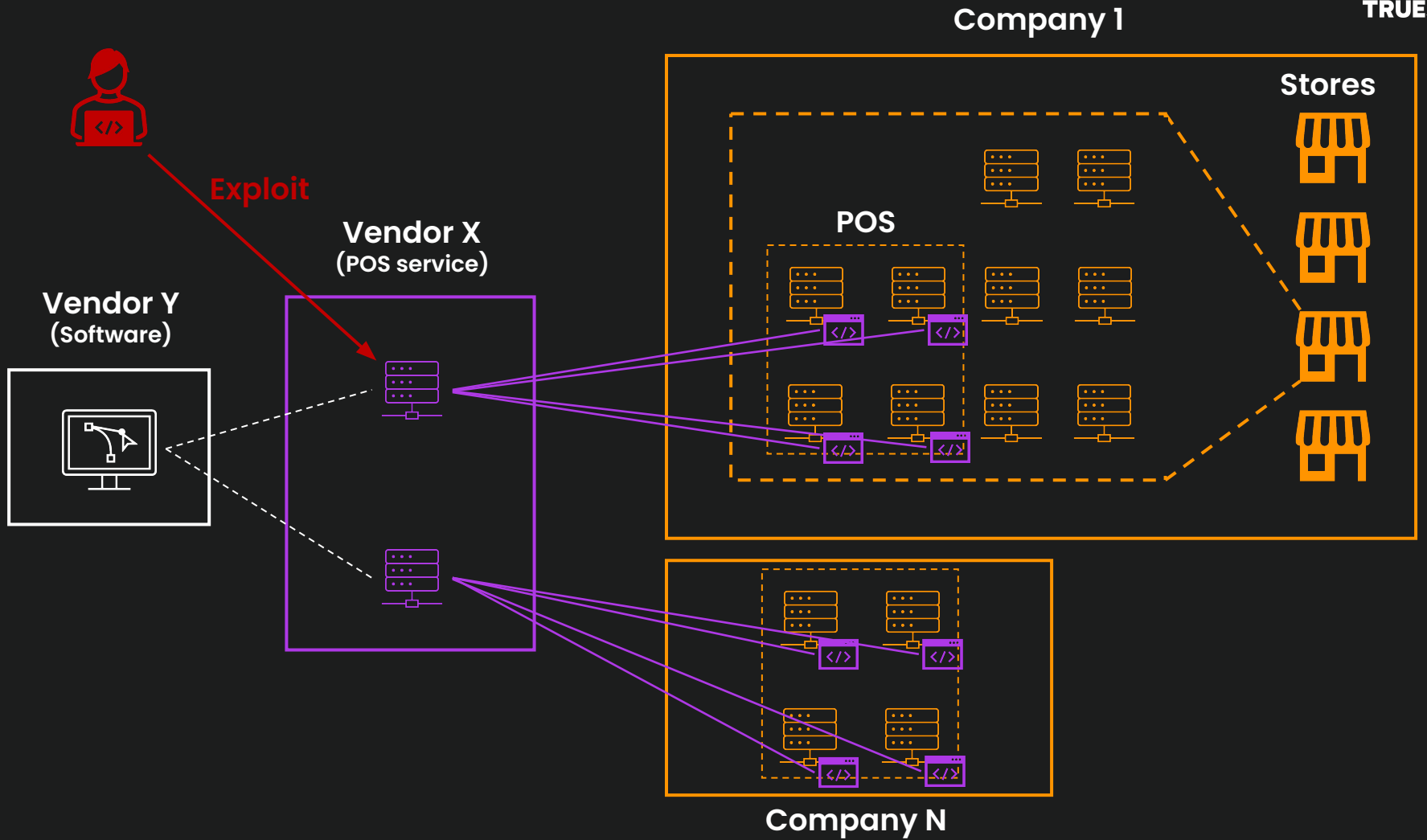
Supply Chain Security in a Connected World

Fabio Viggiani
Hasain Alshakarti

When the breach is not your fault, but your problem

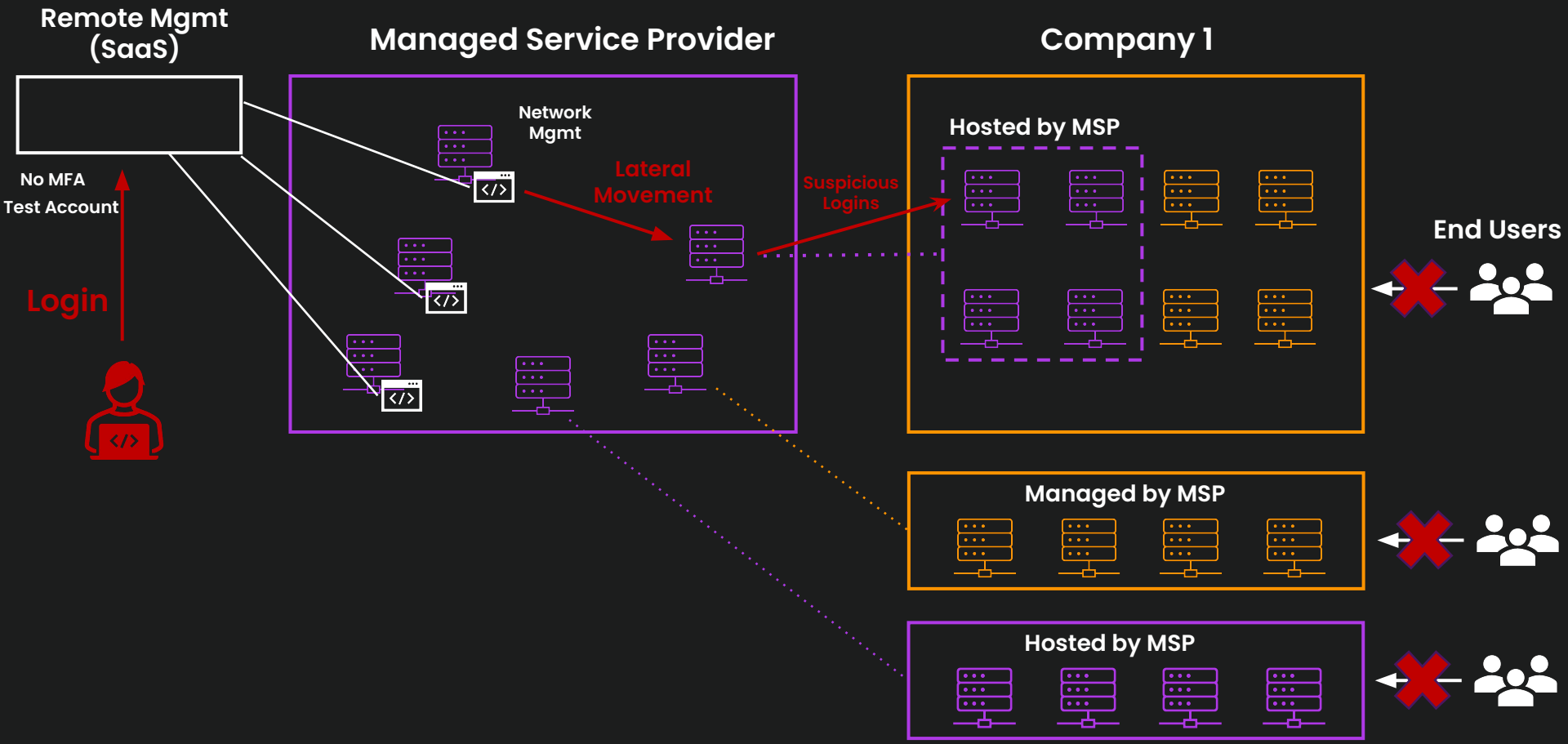
Supply Chain Attacks

- Attacking a trusted third-party vendor who offers services or software to the target
- Software supply chain
- Trusted relationships
- Dependencies and impact
- Highly dynamic and complex ecosystem


Company 1
Stores
POS
Exploit
Vendor X
(POS service)
Vendor Y
(Software)
Company N

Case #1 – Takeaways

- Define availability criticality
- Assess the vendor's capability to ensure availability (incl. setting requirements)
- Review the vendor's remote management solution (hardening, monitoring)
- Assess the software that the vendor uses for remote management


Remote Mgmt
(SaaS)
No MFA
Test Account
Login
Managed Service Provider
Network
Mgmt
Lateral
Movement
Suspicious
Logins
Company 1
Hosted by MSP
End Users
Managed by MSP
Hosted by MSP

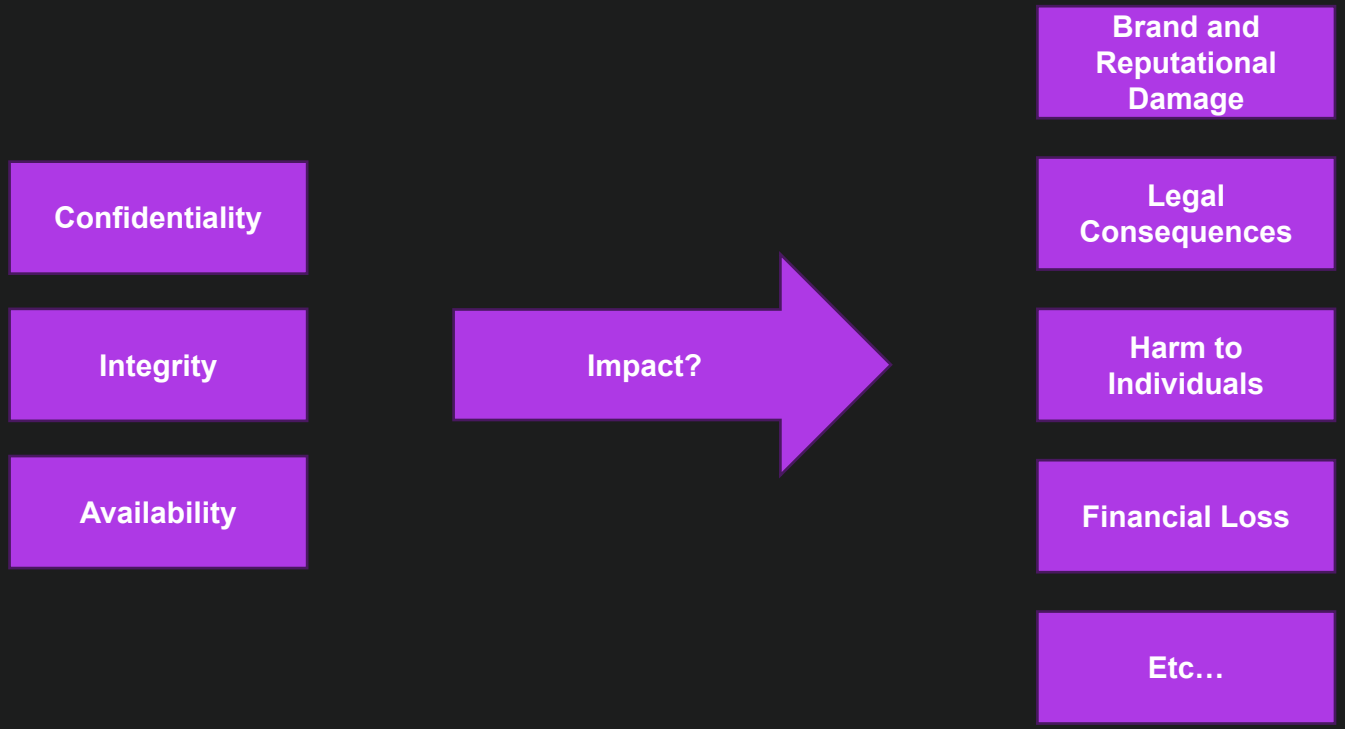
Case #2 – Takeaways

- Although the attack was stopped, the integrity was compromised for all customers and end users
- Ensure immutable backups (or take your own backups)
- Ensure proper monitoring (to be able to verify exactly what files have been modified)
- Fall back solutions towards end customers to ensure availability
- Ensure vendor/MSP has good lifecycle management, patch management, test/prod separation, and other general security hygiene

Securing Your Supply Chain

- Map your systems to your data and functions (incl. dependencies)
- Classify your systems to determine impact

Classify your systems to determine impact



TRUESEC

Value	Brand and Reputational Damage	Legal Consequences	Harm to Individuals	Financial Loss	Etc…
Severe	Severely decreased or lost trust among large group of stakeholders	…	Lives and health of individuals are put at risk	Loss above X	…
Considerable	Decreased trust among a number of stakeholders	…	…	…	…
Minor	Decreased trust limited to one of few stakeholders	…	…	…	…
Insignificant	Minor / temporary decreased trust limited to one stakeholder	…	No or negligible damage to individuals	Loss below X	…

Impact Model

Consequence	Confidentiality Level	Integrity Level	Availability Level
Severe	Strictly Confidential	Critical	Critical
Considerable	…	…	…
Minor	…	…	…
Insignificant	Public	Low	…

System Classification Model

Securing Your Supply Chain

- Map your systems to your data and functions (incl. dependencies)
- Classify your systems to determine impact
- Prioritize vendors based on system classification
- Assess vendor's security (technologies, processes, security controls, exposure, etc.)
- Assess vendor's financial situation
- Consider legal and contractual aspects
- Monitor vendors for breaches and exposure
- Implement mitigations to reduce the risk to an acceptable level

Thank You!


www.truesec.com


x.com/truesec


linkedin.com/company/truesec