Initial post

by Ashok Kumar Shanmugam - Monday, 27 June 2022, 2:56 AM
Number of replies: 2
Digital Enterprise Definition:

A digital enterprise integrates digital tools and technology into all aspects of its operations to improve productivity, customer experience, and business processes.

A digitally modernized company uses cutting-edge technology to stay relevant and surprise customers. From customer experience to operational productivity, technology affects everything. Digital technologies help companies implement new capabilities.

Challenges and Concerns:

Covid-19 boosts online commerce. In 2020's second quarter, 16.1% of retail sales were e-commerce, up from 10.8% the year before. Businesses that already emphasized digital platforms are rushing to develop apps to capture consumer activity online.

Cybercriminals target consumer-tracking companies. In 2019, the FBI received 1,300 online crime complaints per day, up 40% from 2018. Businesses can expect internet-based crime to rise as fast as online commerce in 2020.

Cybersecurity has risen to the top of risks companies face in a digital economy, so they must increase their security protocols. (Mark Schlesinger, 2022).

Buffone says that retailers should run their security operations in an omnichannel way. With the breakdown of barriers between brick-and-mortar and online retail and the rise of programs like BOPIS (buy online, pick up in store), Buffone says that a similar, all-encompassing approach is needed to merge security strategies from both types of retail.

Yes I agree with their views.

References:

1. Theecmconsultant.com (Feb 2022) What is Digital Enterprise? Available at: **https://theecmconsultant.com/digital-enterprise/** [Accessed June 24 2022]

2. Mark Schlesinger (2020) A Growing Digital Economy Means More Cybersecurity Challenges. Available at: **https://www.forbes.com/sites/forbestechcouncil/2020/11/30/a-growing-digital-economy-means-more-cybersecurity-challenges/?sh=6b51d462470a** [Accessed 24 June 2022]

3. Goboomtown.com (October 17, 2019) Protect your website. Available at: **https://www.goboomtown.com/blog/experts-security-threats-retail-tech** [Accessed 25 Jun 2022]

Maximum rating: -
PermalinkReplyExport to portfolio

In reply to Ashok Kumar Shanmugam

Peer Response

by Rob Mennell - Tuesday, 28 June 2022, 2:08 AM

Ashok, thank you for highlighting the cybersecurity concerns emerging from a greater volume of online retail transactions. You also make an important point: many businesses rushed their development of applications and platforms in response to the COVID-19 pandemic (Geer, 2021; Linthicum, 2021; Security Compass, n.d.; Stone, 2021). Developers were pressured to release applications and security patches to meet a timeline, as opposed to completing testing and vulnerability analysis (Security Compass, n.d.). This also led to a unique phenomenon where approximately 25% of zero-day patches produced in 2020 were the result of insufficient investigation; in other words, approximately one third of all zero-day patches failed to identify the root cause of the exploit (Stone, 2021). Because of this, attackers have been able to make minor tweaks to exploits to circumvent security patches (Security Compass, n.d.; Stone, 2021).

Like many of us, I witnessed this with many of the collaboration and virtual meeting software pushing out glitchy patches to keep up with demand!

Thanks for your post, Ashok,

Rob

References

Geer, D. (2021). *Rushed digital transformation is creating security risks*. [online] Hewlett Packard Enterprise. Available at: https://www.hpe.com/us/en/insights/articles/rushed-digital-transformation-is-creating-security-risks-2111.html. [Accessed 27 Jun. 2022].

Linthicum, D. (2021). *The pandemic-driven rush to cloud is compromising security*. [online] InfoWorld. Available at: https://www.infoworld.com/article/3612245/the-pandemic-driven-rush-to-cloud-is-compromising-security.html. [Accessed 27 Jun. 2022].

Security Compass. (n.d.). *Google: Insufficient and rushed patching leads to more zero-day exploits*. [online] Available at: https://www.securitycompass.com/in-the-news/google-insufficient-and-rushed-patching-leads-to-more-zero-day-exploits/ [Accessed 27 Jun. 2022].

Stone, M. (2021). *Project Zero: Déjà vu-lnerability*. [online] Project Zero. Available at: https://googleprojectzero.blogspot.com/2021/02/deja-vu-lnerability.html [Accessed 27 Jun. 2022].

PermalinkShow parentReply

In reply to Ashok Kumar Shanmugam

Re: Initial post

by Amit Pahuja - Tuesday, 28 June 2022, 6:22 AM

Hello Ashok,

I really liked your different insightful post covering digital enterprise and Cyber challenges to bricks and mortar SME wanting to go digital.

You rightly pointed out that “Cybercriminals target consumer-tracking companies.”

It ultimately comes down to usable data for attackers. What could be more beneficial than obtaining unauthorized access to financial services like credit cards or the user's personal information, such their Social Security number.

Small and medium-sized businesses typically have limited resources and a lack of security awareness. This provides an advantage to cybercriminals because the individuals in question are more likely to fall for phishing scams.

Thanks and Regards

-amit

Peer response

by Ashok Kumar Shanmugam - Wednesday, 29 June 2022, 3:03 AM

Hello Gokul,

I liked your detailed post, and more importantly highlighting the mobile security threats.

Mobile security protects smartphones, tablets, and laptops using strategy, infrastructure, and software. Mobile device cybersecurity includes protecting device data, endpoints, and networking equipment. As mobile devices replace desktops, attackers will target them more.

Why Is Mobile Security Important?
As more people travel and work from home, mobile devices have become more common, even among corporate employees. Internet use was once limited to desktops, and only travelling employees had laptops. Mobile devices are the preferred way to browse the internet, and mobile traffic has surpassed desktops.
Mobile devices have a larger attack surface than desktops, making them a bigger security threat. Mobile devices are vulnerable to physical and virtual attacks, but desktops are immobile. Administrators must worry about physical attacks (theft and loss) and virtual threats from third-party apps and Wi-Fi hotspots (e.g., man-in-the-middle attacks). Administrators can better control network and endpoint security on stationary desktops. Users can root, add, and lose mobile devices.

Reference:
Proofpoint.com why is mobile security important. Available at: https://www.proofpoint.com/us/threat-reference/mobile-security [Accessed 27 June 2022]
Maximum rating: -

- **◀ Initial post**
- **Initial Post ▶**

- [redacted]

[redacted]