Case Study

Kiosk industry catching up with changing security challenges and landscapes

Background

Self-serve kiosks have long played an important role in the banking industry for cash withdrawals, deposits, gaming casinos for ticket redemption, loyalty rewards, bill breaking and token and even at airports for self check-in and luggage tagging. The wide acceptance of these technologies for banking activities among consumers has impacted foot traffic in branches and critically important for branch transformation. As customers gravitate towards new technologies that provide 24/7 facility, flexibility and control over their transactions, financial institutions will need to adapt self-serve technology to meet customer expectations even in remote areas.

Challenge

Financial institutions and banks with retail licences are consistently looking for means to increase customer loyalty and satisfaction through better quality of service and convenience. The challenge to increase productivity through automation provides a perfect scene to increase more kiosks. Kiosks can completely if not all, replace common over-the-counter services. However, this may prove otherwise to those who have manage the security aspects since every new kiosk added would mean increasing the surface of attack to the backend servers. Kiosks would become a honey pot for attacks since many financial services will be remotely accessed and transacted - be it physically or through the connectivities between kiosks and backend servers.

Industry

Banking & Financial
Self-serve Kiosks

Challenges

- Allow customers to complete various day to day transactions, traditionally handled by a teller, without assistance at any time of the day, providing extra piece of mind.

Goals

- Increase efficiency, productivity and customers' banking experience through automated self-serve kiosks.
- Minimizing the risk of attack to the banking core network.

Solution

SE*desk*™ is a unified workspace providing secure remote access and isolation suitable for financial services on self-serve kiosks, reducing the surface of attacks in a perimeterless digital workplace.

Solution

Airports, Automated Banking Lobbies, Casinos, Fast Food Chains etc - Self-serve kiosks have become a common sight in many service-based industries. Many of these communications between kiosks and the backend servers have little or no security when sending personal details of users like identity card numbers, home addresses, credit cards, contact details, as well as details about user activity, unencrypted over publicly accessible internet. In a recent example, a couple of white-hat researchers, #Dylan and *Me9187, discovered that a unauthenticated reward server was directly connected to the kiosks on the casino floor and the API which the kiosks were using was wide open and extremely vulnerable to criminal abuse (no SSL protection, API wide open, possibility to identify kiosks by their MAC address…) and through the use the unsecured API to change details, track users and add credit to user accounts and even spin up a kiosk on a virtual machine in order to have your own personal kiosk at home.

In this scenario, SE*desk*™ finds it perfect place as being the right combination of remote access and network layer protection by isolation. By defining a controlled perimeter, SE*desk*™ not only provides authenticated service isolation but also data protection through delivery and storage leveraging the SE*link*™ technology to protect data transfer from the remote self-serve kiosks to the backend server in the control room (without the need for VPN connection). A multi-layer approach to protect both the network and the endpoints from data exfiltration. In addition, it is no longer needed to run native applications and updates on every kiosks as it is centrally at the core. SE*desk*™ immediately reduces the surface of attack and enables major savings in operational costs (updates no longer needed at each kiosks, less downtime).

Benefits

- **Complete isolation** of data and applications on self-serve kiosks
- **Fine-grained access control** to the core enterprise network through context-based policies and User-Kiosk-Server multi-factor authentication
- **Reduced maintenance** on self-serve kiosks
- **Zero configuration** on self-kiosks for easy deployment (VPN free)
- **Optimisation of operational costs**
- **Future proof technology,** ready for resilience against quantum computer attacks

#https://twitter.com/degenerateDaE
*https://twitter.com/Me9187

About Blu5 Group

Blu5 takes pride in supporting digitisation teams in the challenge to reduce surface of attacks, while securing core critical operations. We engineer hardware and software to address the needs of Critical Infrastructures, IoT, FinTech, BioMedical, Space & Defence. Resilience is our team keyword. Cost effectiveness, smooth system integration and timely solutions are our daily leads, working hand in hand with our customers to deliver user friendly implementations suitable for their IT infrastructures. Since foundation in 2007, the Blu5 R&D team, rich of 40+ patents, has been the company’s key enabler for generating innovative solutions.

Blu5 Group
info@blu5group.com
www.blu5group.com