New-Tech Magazine

September 2018 Issue

Now, More Than Ever, Your Organization Needs Strong Authentication

Multi-factor Authentication Tools Reduce Internal Threats and Help Save Patient Lives

Desktops around the globe remain vulnerable to internal attacks and data breaches. Even companies vigilant in taking precautions to protect the desktop are exposed to financial loss, fines, and bad publicity that diminishes their standing on the world stage. Whether through sabotage or criminality, a data breach has the power to send the largest of corporations to the smallest mom-and-pop into bankruptcy. Recent implementation of the EU's GDPR drives the point home further: It is in the best interest of all companies to deploy the latest technological tools that stave off unauthorized access, avoid breaches of private data, and keep their organizations ahead of the curve.

What are the internal threats companies face going into 2019? Surprisingly, many of the same threats they've faced since the advent of the personal computer. Viruses, trojans, lost and stolen passwords, and unauthorized access to data, to name a few. Employers who have not established sound, forward-thinking desktop security policies and strategies, that take into consideration every level of operations, are faced with cleansing the aftermath of lost, shared, or stolen passwords. They're faced with the headache of password management. They're left to deal with the aftershock of unauthorized data access. In the case of patient care, they could very well be held responsible for the improper dispensation of drugs that results in loss of life and the monetary damages that follow.

With so much at stake – money, time, consumer privacy, organizational reputation – this is clearly no time for any entity to remain complacent about desktop security.

Yet, amongst the bad, there is also good news. The large number of products now available to IT professionals presents a robust opportunity to hedge against data loss while enabling seamless app navigation by employees. Today's Single Sign On (SSO) software offers employers the assuredness of foolproof multi-factor authentication along with an increased level of productivity. An employee is no longer required to remember and laboriously enter passwords, or log in separately to each desktop program to maintain network security. A single, no-click sign-on is all it takes for secure access – saving time without sacrificing security. System administrators are in full control of setting policy within the Windows Active Directory to block access to unauthorized users, making data breach by lower level employees much less likely. More and more hospitals and pharmacies around the world are adhering to e-prescribe standards that use SSOs to enroll credentials and identify providers, employing multi-factor authentication for the ultimate accountability. Pioneering companies like Crossmatch, Imprivata, CA Technologies, and Identity Automation have set the standard in creating today's versatile SSO software that responds to the needs of business across all platforms, all sectors.

Peripheral manufacturers have reacted in kind with innovative products of their own. Working in tandem with leading SSOs, security peripherals achieve the highest possible level of access control available today for business – the most sophisticated of which support multi-factor authentication along with other important features that protect the desktop. Biometric fingerprint readers have become a leading solution for foolproof end user authentication. When paired with RFID badge reader technology, security is taken to an even higher level, making it that much harder for potential intruders to gain access. This dual authentication, when combined with sonar presence technology, offers employers the trifecta of desktop security.

In preventing data breach, one of the more important, but sometimes forgotten, aspects of workstation security is logoff. A single unattended computer can leave a company vulnerable to unauthorized access, penetration of confidential information, and stolen intellectual property. Sonar presence technology detects the presence of a user upon approach to a locked desktop, prompts the user to enter security information, i.e., username, password, badge identification, or biometrics – and triggers automatic and secure logoff when a user physically moves away from the workstation.

Keyboards manufactured by Key Source International integrate each of these important features into one compact desktop device. Much more than a superior input vessel, a KSI keyboard integrates no less than four protective, mix-and-match functions into one device, routed through a single USB port: fingerprint biometrics, RFID card reader technology, sonar walk-away presence detection, and a software-driven keyboard cleaning system that controls infection at the clinical desktop on an enterprise-wide basis. An amazing achievement for keeping pace with the ever-increasing demand for physical access control.

At $3.86 million, the average cost of a data breach has increased 6.4 percent globally, according to a 2017 study conducted by IBM Security and Ponemon Institute. With so much at stake – money, time, consumer privacy, organizational reputation – this is clearly no time for any entity to remain complacent about desktop security. Ample software and hardware tools are now at the disposal of every IT professional who seeks to safeguard the network and realize an improved user experience.

KSI Key Source International

Key Source International, located in California, manufactures security keyboards and standalone pods, engineered for healthcare, banking, and government. For more information, visit KSI Keyboards at www.ksikeyboards.com and www.sanakey.com.