BeyondTrust Response to Area #1: Multi-function Consideration for Deployed Software

To help ensure agencies and enterprises align the appropriate security rigor for protection of critical software and help ensure the continuity and integrity of their missions, we must start by defining what constitutes "critical software." In today's enterprise-level environments, "critical software" should be defined by a variety of factors. "Critical" software can be application software, which relates to the software's access to, maintenance of, or transmission of sensitive data; system software, categorized as software that controls and manages networked devices, including directory services, client, server, or network hardware; and public-facing software, which presents unmitigated risk exposure.

The first category, application software, is installed in a client/server configuration or on individual systems as productivity software, such as word processors or spreadsheet manipulators. Software within this category receives its critical designation because it is considered sensitive and/or classified under privacy laws or government designations.

For example, applications that maintain, transmit, or access data governed under the Health Insurance Portability and Privacy Act (HIPAA) should be designated "critical" considering the type of data and the potential for massive damage resulting from a cyber security breach. Similarly, Personally Identifiable Information (PII) is defined by OMB Memorandum M 071616 as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual". This data, as dictated by OMB Memorandums, would create a true potential for harm. In this case, not only is the harm substantive in cost, but it also creates a potential life-threatening risk. Therefore, the same software that is deemed critical in one system may not receive that designation in another simply based on the sensitivity of the data it can access, and may transition from normal operations to a critical designation based on the current state of data being accessed.

In April of 2015, operators at the Office of Personnel Management discovered a breach in personnel management software, including "SF-86" Forms, which contained the extensive background information for cleared civilian personnel working in the federal government. Fingerprints, financial information, known friends and relatives, and job assignments are just a sample of information included in the breach. Multiple sources cited the trove of information as a significant value to the international intelligence community, and a potential significant risk to those employees who might be serving abroad or undercover. This is a clear example of combining sensitive and/or classified data with PII to form a potential for harm.

The second category, system software, provides management for networks, databases, individual systems, and other utilities as necessary for the efficient running of the network. The critical status of system software is determined by the impact to an organization or mission if that software and data were no longer functioning or secure. A particularly sensitive subset of system software includes authoritative directories, which provide the base of authentication for most modern networks. A breach of this software allows threat actors to access almost everything of value on a network and may allow them to regain access in the future. These directories may be the most significant critical piece of software on a network. Database servers are the backbone of the modern Enterprise Resource Planning (ERP) and productivity software. Often containing tens of thousands of data entries, and supporting every known fiscal management software in existence, databases provide the essential platform for conducting business. Operating systems for clients or servers could provide base function access to a system and any activity that occurs on it.

System software that governs network hardware provides a host of security and utility functions to devices once considered the perimeter of the network. Access to this software will grant lateral movement or allow unmitigated access to sensitive data areas. Even as NIST (National Institute of Standards and Technology) and CISA (Cybersecurity and Infrastructure Security Agency) begin to recognize identity as the perimeter, network hardware and the underlying management software still cannot be understated in their importance. These services provide dependent functions for other critical software. Any unauthorized use or breach of this software could render multiple functions inoperable or allow continued access to a set of data otherwise intended to be governed by policy and reputation. In addition, system software such as authoritative directories, can provide privileged access to a multitude of other critical software, allowing for unwanted lateral movement and data exfiltration en masse, potentially resulting in substantive loss of trust and data. Any software that uses a set of privileged credentials to launch or elevate should be considered "critical." Such software packages are vulnerable to an array of attacks attempting to retrieve the credentials or use the elevated access of the application to launch secondary or tertiary malware applications to continue to infiltrate a network or probe for additional attack vectors. Zero Trust architectures for privileges and remote access help resolve some of these security concerns, however, require additional controls to be effective end-to-end.

Additionally, software that is considered "public facing", defined by section 508 as "[software] made available by the agency to members of the general public", provides an extraordinarily vulnerable attack vector into an agency, specifically if the underlying data services also serve internal software or components of the network. Much like a border crossing, these software packages should take precedence as "critical" because their breach could open multiple attack vectors into an agency's network, exposing broader damage as threat actor's probe for opportunities.

Defining "critical software" is a necessary exercise to ensure proper security posture across an agency's network. The factors by which we designate software packages "critical" can vary, but include understanding the types of data it accesses, the level of systems it controls, and/or the open attack surface that it carries. While some software may always be classified as critical, classification can vacillate based on the data being accessed at any given time. Removing unnecessary or risky privileges from any critical software will help mitigate risk.

*Author and proposed speaker: Josh Brodbent, *Sr. Public Sector Security Director*, BeyondTrust
jbrodbent@beyondtrust.com, 870-362-6581