UseCase
City of Bonn

The City of Bonn is building a protective shield against unknown malware code

The 72-meter-high city hall is the headquarters of the municipality of the federal state of Bonn. (Source: Federal City of Bonn)

The protection of confidential data is of the highest importance in the municipality. Here, the municipality of Bonn is going in an innovative direction. By choosing the Bromium solution, it is safeguarding the end devices of its employees and thereby the confidential data of citizens, also from previously unknown malware code.

Traditional security tools have now become standard in communal IT today. New zero-day attacks, advanced persistent threats or also ransomware Trojans cannot be reliably detected with them. This is reason enough for the municipality of Bonn to take on the task of increasing client security. Two aspects were of particular importance: Security when surfing and in email communication. While companies can strictly regulate the reception of email enclosures or access to websites, this is not possible in municipalities due to legitimate citizen concerns. PDFs and ZIP archives must be permitted; employees should be able to visit the relevant forums or access adult sites while supporting the area of youth protection.

An additional challenge lies in the fact that, due to the extensive range of municipal tasks, hundreds of applications, tools and specialized processes must be provided and must be kept runnable.

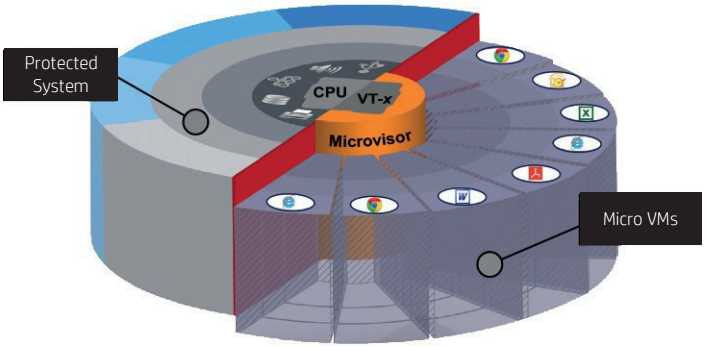
Email and browser protection from one source

When selecting a client security solution, the municipality of Bonn initially considered several applications that address the vulnerability of the Internet browser and allow safe surfing. However, the extremely important topic of email was not covered with such solutions. It quickly became clear that the secure platform of Bromium, with its technical concept of "isolation instead of detection of malware code using micro-visualization" is the correct choice.

As part of a brief evaluation phase, extensive functional and performance tests were conducted. A central result was that around one quarter of the approx. 4,000 computers did not have the required set-up for a seamless use of the Bromium solution. Consequently, a successive rollout of the secure platform in combination with the replacement of older hardware and the introduction of Windows 10 was decided.

Bromium solution relies on isolation instead of detection

The central characteristic of the Bromium solution is that the detection of malware code is not the priority but rather the effective avoidance of its effects. This is implemented through the isolation of all risky user activities, more precisely through micro-visualization. The core elements are a Xen-based hypervisor especially developed in terms of security and the integrated virtual features of all current CPU generations.



Updating features of all current CPU generations. The Bromium solution then always processes tasks in virtual instances if it can be dangerous – i.e., when accessing a website, when opening an email attachment or accessing the data of a USB device. Here each individual task runs in its own micro-VM – and each strictly separated from the actual operating system and the connected network. This thereby precludes the compromise of the end device and the municipal IT network.

"Bromium offered both the technically best solution as well as clearly the most cost-effective solution with the licensing and service model," states Dirk Schumacher, manager of the specialized department IT Security and IT Strategy in the HR and Organizational Office of the Federal City of Bonn.

About Bromium

Bromium, with its headquarters in Cupertino in the Silicon Valley, is a pioneer in the area of application isolation using micro-visualization. Unlike conventional solutions, Bromium does not rely on the recognition of malware code but rather prevents its effects: Malware of all kinds, regardless of whether it is from the web, emails or USB devices, remains safe because every user task is run in a hardware-isolated micro-VM. Bromium can then prevent the operating system from being compromised.

Further information at www.bromium.com.

June 2020 – 4AA7-7797ENW