Case Study

AEOS increases security at ING's BE branch offices.

{ Security management in banking is a discipline unlike any other. Rather than integrating all security into one centralized system, some banks choose decentralized security for their branch offices. AEOS, a leading platform in integrated security, turns out to be just as effective when deployed decentrally. }

"We were already using Nedap AEOS in our headquarters, as well as various regional offices. Then, in 2011, the security system used by our 800 branch offices in Belgium needed to be extended with access control. Because we were already aware of AEOS's capabilities and very satisfied with its performance, it was a logical step to ask Nedap to solve our problem."

Joris de Greve, Security Manager at ING Belgium.

ING

Autonomous systems.

ING's 800 branch offices in Belgium were already equipped with autonomous intrusion detection and camera surveillance. All doors and their accessories, such as locks, push buttons and door contacts, were monitored and controlled by the intrusion detection system. Doors were opened and closed using keys in security cylinders. A central alarm management system handled alarms coming in from local intrusion control systems.

Key management had become a problem, according to De Greve. "It was virtually impossible to keep track of the physical keys and who was authorized to use them. We had no central database in which authorizations could be assigned or retracted."
In addition, changing locks, replacing keys and keeping key plans up to date had become difficult. "It was time for an electronic access control system," explains Peter Rommens, Country Manager at Nedap Belgium. "Since all peripherals were connected to the intrusion detection system, the scope of the project was clearly defined. We were looking purely at access control at one or more doors per office."

nedap
technology that matters

Cliquez sur «Prenez rendez-vous» sur www.ing.be
ING
Klik op "Maak een afspraak" op www.ing.be
ING

Narrowing it down.

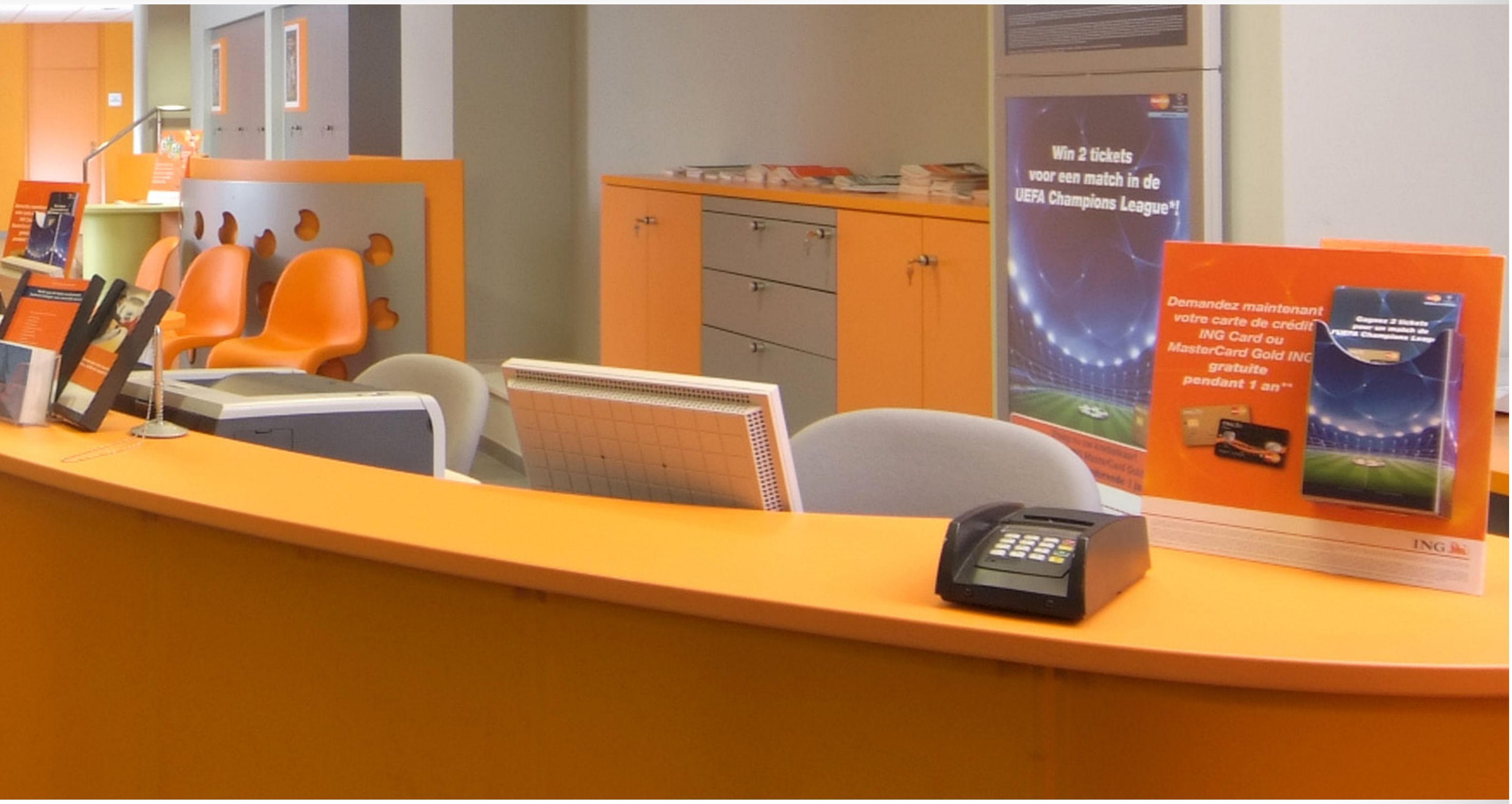
After considering a wide range of solutions, ING eventually selected two for further evaluation. One was to add access control to the existing intrusion detection systems. This was technically the least complicated option, because the basic infrastructure and necessary hardware were already in place. The other option was to expand the centralized AEOS system that was already up at headquarters and regional offices to include access control at the branch offices.

The latter offered the major advantage of being able to connect all branch offices to one central database, while retaining the ability to delegate responsibility for authorizations to lower-level security management layers. Other benefits of this option included its system architecture, the proven stability of the system for large numbers of offices and cardholders, the system's scalability and flexibility, the native IP controllers' ability to communicate peer-to-peer and bypass the server, and the system's redundant facilities and security (failsafe, switching servers, etc.).

Flexible and extra secure.

The factor that clinched the deal was that AEOS allowed for decentralized management of separate units and the use of entrance filters. This meant local offices could be authorized to manage their own security without access to other offices' data, Joris de Greve explains. "The bank's security structure is based on central access to buildings and central facilitation of technical solutions, but decentralized security and access responsibility per zone. Therefore, the system must allow us to cluster cardholders into groups with different authorizations. AEOS supports this."

"Another factor was ING's requirement that authorizations not be assigned to a badge, but to a cardholder," adds Rommens. "This builds in extra


Win 2 tickets voor een match in de UEFA Champions League*!
Demandez maintenant votre carte de crédit ING Card ou MasterCard Gold ING gratuite pendant 1 an**
ING

security: cardholders who lose or forget their badge are issued a replacement while the original badge is invalidated. This guarantees there are no unaccounted-for, authorized badges 'floating around'.

Decentralized approach.

ING combines centralized and decentralized policies. Overall security policy is set at top headquarters; security management there decides who is authorized to manage accounts and which authorizations may be assigned. This is part of the bank's security structure. We ask ING Belgium Security Manager De Greve to illustrate.

"For example, the Milan office uses a server in Belgium and the technical facilities provided by central security management. However, the management in Milan are in full control of who is allowed access to their building and when," he says.

User training is also decentralized. There are some 500 administrators, all of whom were trained internally and decentrally. AEOS enables this flexibility. Because AEOS is web-based, interventions are simply and swiftly carried out.

Keeping an eye on things.

A consequence of decentralization is the need for reports. "Central management wants to keep an eye on what is happening at the various branch offices," De Greve says. "Is security functioning properly? And are offices complying with security policy?" He believes reports "are also a valuable management tool." For example: how many people are at work at any given time, or whether people only come in a few times a week. "This helps us to make sound decisions concerning flexible office space, for instance, and that's an important way to reduce costs."

Proxy offices roll-out.

ING BE has two different types of offices: Proxy offices where all money is distributed by ATMs and Full Service where staff behind counters provide service. In both types of branches local staff is present and mobile specialists are available to respond to specific needs or questions customers may have. Nedap is currently installing AEOS at the 800 Belgian branch offices at an approximate rate of nine offices per week.
Peter Rommens explains how the roll-out is being organized logistically: "In preparation for installation, ING centrally creates the appropriate authorizations in AEOS. Then, Nedap's business partner defines the configuration and uploads this to the controller. This means on-site installation is quick; once the controller is connected and deployed, the system is up and running."

AEOS at proxy offices.

"The bank preferred our proposed solution, with one AP4803x per branch office, over a solution with one or more AP6003 network controllers per office but only one AEpu per ten offices," Rommens says. "Although having one AEpu per office is costlier, availability is more sure with the AP4803x and it offers more long-term advantages. It means each office is prepared for expansion of its access control or the addition of other security functionalities."
Proxy offices are defined as individual access control zones. Each office has its own profiles defining who is allowed access and on what basis. Proxy offices are secured with readers and a key replacement badge. The alarm system runs separately from the access control system. The badge only provides access, while arming and disarming the alarm system requires identification. In line with existing policy, if an unauthorized person finds a badge and tries to use it when the office is empty, this sets off an alarm. If a person tries to use a stray badge when the office is manned, he or she is immediately exposed by staff (social control).

"Badges are also blocked based on expiry date or end of contract because in general the fewer badges in circulation and the fewer people with access, the smaller the security risk," says De Greve.

Key Figures.

- Licence for 25,000 badges, 1,000+ access points
- Oracle DB application server
- Backup server
- Test server
- Linked with HR database (Peoplesoft) for importing data
- Use of rule engine to automatically change authorizations
- Hardware AP4803 + Convexs/Invexs readers