N°3 – Octobre 2018 News

Etablissements de santé

Edito - L'obsolescence

Le sujet de l'obsolescence programmée pour les produits grand public est à la mode. Mais le sujet de l'obsolescence naturelle est tout aussi important dans notre secteur.

La sûreté est à la convergence de l'informatique, de l'électronique et de la quincaillerie (menuiserie, huisserie, etc.). Or les deux premières citées sont des modèles d'obsolescence technologique. Un PC sous Windows XP ne pourra plus accueillir une nouvelle version de votre logiciel favori et le remplaçant de Windows XP vous forcera à remplacer votre PC. C'est un processus bien connu qui fait la fortune des fournisseurs de ces produits depuis le début de l'informatique.

Dans le contexte de la sécurité, il faut également faire face à l'intelligence des hackers qui contribuent à l'obsolescence par exemple des outils d'identification. Le code barre masqué ou la piste magnétique ont laissé leur place au badge sans contact Mifare qui est lui-même en train de laisser sa place à son cousin, le badge Desfire. En attendant qu'il soit nécessaire de diffuser une technologie encore plus solide.

Nous consacrons plus d'un tiers de nos efforts de R&D, non pas à développer de nouvelles fonctionnalités mais à garder la solution existante compatible avec les nouveaux environnements informatiques, logiciel et matériel, à faire face à la disparation de certains composants électroniques remplacés par une nouvelle génération, ou même des décisions d'éditeurs de ne plus soutenir une technologie incontournable quelques années auparavant (applet Java par exemple).

Dans le même temps, une solution de contrôle d'accès installée voici cinq ans voire dix ans continue habituellement de fonctionner sans soucis. Les logiciels sont éprouvés et l'électronique des lecteurs et des cartes particulièrement résistantes.

C'est donc souvent une mauvaise surprise que de découvrir, le jour où une extension est nécessaire, ou qu'un composant tombe en panne, que le remplacement de la pièce du puzzle, n'est plus aussi simple et que de fil en aiguille, plusieurs composants de la solution sont à mettre à jour.

Comment s'y préparer ? sachant que l'on ne pourra l'éviter !

- Anticiper un budget annuel de remise à niveau du parc. Une partie, comme la mise à jour des logiciels pourra être incluse dans un contrat de maintenance, mais pas le remplacement de vieux PC ou de composants électroniques trop âgés
- Être informé du statut des produits de votre installation et pour cela ARD va rendre plus aisé l'accès aux dates d'obsolescence de ses produits
- A chaque projet d'extension de votre configuration, ou bien lors de l'introduction de fonctionnalités supplémentaires, il convient de vérifier qu'il n'y a pas quelques composants qui sont à remplacer pour mener le projet à terme. Les équipes d'ARD sont disponibles pour aider à faire cette analyse.

Frédéric Spagnou - Président

Carte A2 : ancienne génération d'UTL ARD

ARD - Micropolis, Bâtiment Clématis, CS26003, 05005 GAP CEDEX France
Tél. : 33 (0) 492 525 800 - Fax : 33 (0) 492 525 801 e-mail : contact@ard.fr – www.ard.fr

Etablissements de santé

Bonnes pratiques

Bien gérer les listes noires en présence de serrures autonomes.

Les usagers de votre contrôle d'accès peuvent perdre leur badge, ça arrive parfois, fréquemment même en milieu scolaire !

Dès qu'un évènement de ce type est signalé, il faut écarter la menace de ce badge perdu ou volé et qui pourrait être utilisé à l'insu de son propriétaire. Le gestionnaire du système de sécurité met donc le badge en opposition dans le logiciel de contrôle d'accès, ce qui a pour effet immédiat de le rendre inopérant sur tous les points d'accès, la menace est donc ainsi écartée. Enfin pas vraiment, en particulier si votre contrôle d'accès comprend des serrures électroniques autonomes (non connectées).

S'il est incontestable que les serrures autonomes présentent de nombreux avantages (coût, simplicité d'installation, etc.), elles nécessitent une attention particulière de votre part.

Tout d'abord, il est important d'avoir à l'esprit que les droits d'accès à ces serrures autonomes sont inscrits dans la puce RFID du badge de l'utilisateur et non dans le matériel.

Les constructeurs de serrures ont bien entendu prévu le cas d'un badge perdu ou volé, ainsi, si la serrure dispose de la liste des badges en opposition (ou liste noire) dans sa mémoire interne, l'accès de ces badges sera refusé.

Il convient donc de transférer l'information aux serrures car ceci ne peut pas être fait en temps réel et à partir du système central puisqu'elles ne sont pas connectées.

Par défaut, il y a le mécanisme de propagation virale : l'information du badge banni se propage à l'ensemble des serrures au fur et à mesure des badgeages des autres utilisateurs de votre site. C'est une solution attirante sur le papier mais qui ouvre une faille béante dans votre système de contrôle d'accès puisque vous ne maîtrisez pas le moment à partir duquel le badge en liste noire sera bien reconnu comme tel par toutes les portes auquel il avait précédemment accès.

Cette solution peut convenir lorsqu'il s'agit de badges non restitués par des personnes de confiance mais surtout proscrire s'il y a une quelconque suspicion de vol.

La solution la plus sûre est donc d'intervenir physiquement devant chacune des serrures sur lesquelles le badge à mettre en opposition avait des droits et mettre à jour la liste noire de ces serrures en présentant un badge administrateur contenant cette information.

Intégration ARD offline : transport de liste noire par une carte d'admistration

Tout est maintenant pour le mieux dans le meilleur des mondes. Sauf que les serrures électroniques ne disposent pas d'un même espace de stockage que vos ordinateurs. Elles permettent de gérer des listes noires allant de quelques dizaines à une centaine de badges tout au plus. Attention donc à ne pas atteindre ces limites car vous seriez dans l'impossibilité d'en ajouter des nouveaux !

Quelques bonnes pratiques vous éviteront la plupart de ces problèmes :

- Donnez systématiquement des durées de validité raisonnables aux badges qui portent des droits sur des serrures autonomes. Si vous donnez des durées de plusieurs années, la serrure sera contrainte, en effet, de garder le badge en liste noire jusqu'à l'extinction de ces droits !
- Soyez assez convaincant pour que les personnes qui n'ont plus besoin de leur badge (départs, absence de longue durée, …) les restituent afin de ne pas alourdir inutilement la liste noire.
- Privilégiez la propagation de votre liste noire par la carte d'administration plutôt que par viralité. Et n'utilisez la propagation virale qu'avec parcimonie, uniquement dans un contexte maîtrisé qui ne créera pas de faille de sécurité.

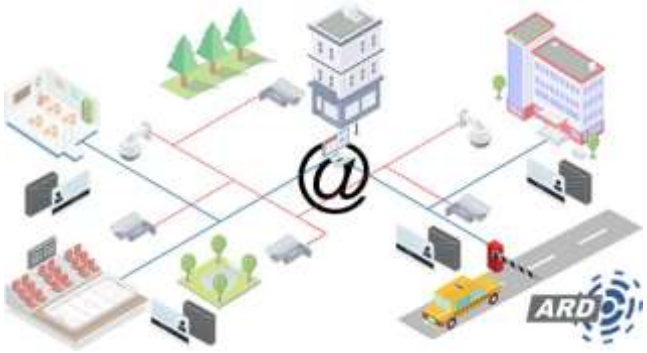
ARD - Micropolis, Bâtiment Clématis, CS26003, 05005 GAP CEDEX France
Tél. : 33 (0) 492 525 800 - Fax : 33 (0) 492 525 801 e-mail : contact@ard.fr – www.ard.fr

N°3 – Octobre 2018 News

Etablissements de santé

Contrôle d'accès et internet

Avec les solutions de contrôle d'accès ARD Access et ARD Ace, les architectures sont dites « client léger », dans le sens où il n'est pas nécessaire d'installer le logiciel de contrôle d'accès « client » sur un PC, un simple navigateur web suffit pour pouvoir l'exploiter à l'image d'un site internet.



Une pratique courante sur les sites sensibles consiste à isoler du point de vue réseau l'ensemble de la solution. Mais ce n'est parfois pas possible et dans ces cas-là les postes d'exploitation ont probablement accès à Internet où à la messagerie, ce qui les expose à des risques de sécurité permanents tels que virus, cheval de Troie ou attaque d'un hacker.

En reprenant les termes de l'ANSSI, le respect d'une « hygiène informatique stricte » sur les postes de travail est crucial, il passe par une gestion rigoureuse des pares-feux, comptes utilisateurs, politique d'authentification, antivirus et mise à jour régulière des correctifs.

Et c'est précisément sur le dernier point que nous souhaitons attirer votre attention. Le système d'exploitation, votre navigateur web et certains de vos logiciels seront automatiquement mis à jour avec de nouvelles versions, souvent sans même vous en demander l'autorisation (en fonction de vos paramètres).

Certaines fonctionnalités du logiciel de contrôle d'accès qui fonctionnaient parfaitement la veille, peuvent ne plus fonctionner le lendemain !

Il est très difficile d'anticiper l'impact de ces correctifs sur les applications car les éditeurs de navigateur web ne prennent pas le temps d'informer à l'avance les éditeurs de logiciels comme ARD.

Nous surveillons régulièrement la compatibilité de nos applications avec les évolutions des navigateurs web les plus répandus sur le marché, mais certaines de ces évolutions entrainent le développement et tests de correctifs qui ne sont pas immédiatement disponibles.

Vous comprendrez, au vu de ces lignes, qu'ARD préconise :

> D'éviter, lorsque c'est possible, de laisser les postes d'exploitation du contrôle d'accès ouverts sur Internet.
>
> De maîtriser les mises à jour de vos logiciels, en particulier les navigateurs web, en les appliquant manuellement après avoir vérifié la compatibilité avec votre système en place.

Votre contrat de maintenance vous donne accès à la hot line ARD, alors si vous êtes confronté à un problème de ce genre, contactez-la par téléphone au 04.92.52.48.00 ou par @mail à l'adresse sav@ard.fr.

Actualités Clients

De nouveaux établissements de santé ont choisi nos solutions, parmi eux :

Les centres hospitaliers Broussais à Saint-Malo (35) et Abbeville (80) ainsi que l'Adapei le Tampon (97 Réunion).

D'autres ont fait évoluer leur installation :

La clinique du parc à St-Ouen l'Aumône (78), les centres hospitaliers de Mulhouse (68), Bastia (2B), Saint-Pierre (Réunion 97) et Rouffach (68).

ARD - Micropolis, Bâtiment Clématis, CS26003, 05005 GAP CEDEX France
Tél. : 33 (0) 492 525 800 - Fax : 33 (0) 492 525 801 e-mail : contact@ard.fr – www.ard.fr

Etablissements de santé

Agenda

HOPITECH

ARD était exposant aux journées d'étude et de formation HOPITECH 2018 à Paris La Défense du 10 au 12 octobre.

Dans le cadre du forum Tech-innov, les stagiaires ont pu écouter Germain Dupont, Responsable commercial pour l'Ile de France, présenter les solutions de sûreté ARD destinées aux professionnels de santé.

Il a rappelé que le contrôle d'accès ne se résumait pas à la fourniture de badges d'accès et de serrures électroniques et en vue de remplacer les clés et cylindres mécaniques traditionnels. La dimension sécuritaire est un élément important à prendre en compte, encore plus dans le contexte d'un établissement de santé où la sensibilité de certaines zones exige une sécurité forte (pharmacie, labo, etc.).

En effet, un système de contrôle d'accès doit garantir la traçabilité des accès et offrir toutes les fonctions visant à limiter la vulnérabilité du dispositif comme par exemple la gestion efficace des listes de cartes en opposition ou la supervision de l'installation. Le système doit permettre à l'opérateur de sécurité d'être informé lorsqu'une porte est ouverte trop longtemps ou lorsqu'une tentative d'intrusion ou d'agression a été détectée. Une véritable solution de sureté doit mixer les dispositifs de contrôle d'accès, de détection et de vidéosurveillance.

Mais ce n'est pas suffisant, il faut également pouvoir affecter facilement les bons droits d'accès aux bonnes personnes, si possible de manière automatisée en interfaçant le système de sureté avec le système d'information de l'établissement.

En tant que fournisseur de solutions, ARD sait mettre le bon produit à la bonne place, qu'il s'agisse d'un produit issu de la gamme ARD ou celui d'un fabricant tiers.

Une solution intégrée est capable d'intégrer les dernières innovations en matière de dématérialisation des identifiants : le badge traditionnel (carte CPS, Carte établissement) remplacé par le smartphone dans les bâtiments et la lecture de plaque minéralogique au parking.

Expo PROTECTION
LE SALON DE LA PRÉVENTION ET DE LA GESTION DES RISQUES

6 > 8 NOV 2018
PARIS PORTE DE VERSAILLES
PAVILLON 1

Nous vous attendons à Expo-protection, du 6 au 8 novembre, à Paris Porte de Versailles – Pavillon 1 – stand D094.

Nous vous accueillerons au sein de deux espaces, l'un dédié à notre solution de sureté intégrée ARD Access et le second consacré au logiciel de contrôle d'accès ARD Ace lancé l'an dernier à l'occasion du salon APS.

Vous découvrirez nos dernières nouveautés en matière de supervision graphique, contrôle d'accès, détection intrusion, vidéosurveillance, interphonie, gestion des cartes et cartes virtuelles, gestions des visiteurs par QRCode, intégration des béquilles et cylindre offline et online Apério V3, etc.

Si vous souhaitez une démonstration approfondie ou bien rencontrer spécifiquement l'un de nos collaborateurs présents au salon, indiquez-nous par Email la date et l'heure approximative de votre arrivée, nous prendrons les dispositions pour vous réserver le meilleur accueil.

Etablissements de santé

Actualités produits

ARD Access, à partir de la version 1.9.x

L'interfaçage avec le dispositif anti-intrusion Galaxy Dimension a été entièrement remodelé : la déclaration du matériel et de la configuration Galaxy dans ARD Access est facilitée via l'import d'un fichier XML contenant les points d'intrusion, zones, centrale, etc. La supervision n'est pas en reste, la communication avec la centrale et les alarmes intrusion sont remontées, de même que la mise sous et hors alarme et l'éjection de points sont désormais possible avec ARD Access.

La supervision des évènements APERIO Online L100 a été améliorée : en complément à l'état des piles et à la communication, l'état de la porte (verrouillée, déverrouillée et ouverture trop longue) et les défauts mécaniques (effraction, blocages mécaniques) sont remontés en supervision. L'ouverture à distance depuis un écran de supervision est désormais opérationnelle.

Mais aussi :

- L'enrichissement de l'API de Webservice SOAP d'ARD Com : listes d'oppositions, calendrier des jours spéciaux, accès à l'historique d'évènements.
- La création des groupes prédéfinis « Agent de sûreté », « Exploitant », « Responsable sûreté » ou « Administrateur ».
- Des améliorations ergonomiques diverses, de nouveaux objets d'animation pour les synoptiques de supervision (portail coulissant, lecteur online, etc.), stabilisation de l'interface du terminal Oterm Touch.
- Une bibliothèque de connecteurs de provisioning enrichie : Heberg3, système de gestion de l'hébergement pour les CROUS, Gestion des clés Traka, connecteur de synchronisation entre plusieurs instances d'ARD Access, etc.).
- Gestion d'un identifiant secondaire (ex : identifiant encodé dans une application de la carte et identifiant n° de série de la carte).
- Intégration finalisée du format OSS sur carte Desfire (serrures électroniques Apério Online V3).
- Intégration du dispositif LAPI Tattile pour la lecture de plaque minéralogique.
- Nouveau firmware pour nos lecteurs, plus performant, configurable pour s'adapter aux différents mapping de cartes à puce rencontrés.

ARD Ace, à partir de la version 1.2.3

Divers assistants et améliorations ergonomiques ont été apportés dans cette version, une attention particulière a été consacrée au programme setup d'installation, l'objectif étant d'éviter de devoir faire appel à un spécialiste système et réseau pour installer ARD Ace.

Mais il y a aussi de nouvelles fonctionnalités telles que les serrures électroniques Apério offline V3 au format OSS sur carte Mifare, les serrures électroniques online Smart Intego de Simons Voss et l'anti-retour temporisé (le passage d'un usager à un point d'accès n'est possible que si l'intervalle de temps avec le passage précédent est supérieur à une valeur paramétrable).

Ace propose également un connecteur de provisonning de données au format CSV, il permet d'alimenter la base de données des usagers et des badges automatiquement, un gain de temps évident pour le gestionnaire.

Enfin, Ace permet l'utilisation des cartes régions pour les lycéens de Rhône Alpes Auvergne.

ARD - Micropolis, Bâtiment Clématis, CS26003, 05005 GAP CEDEX France
Tél. : 33 (0) 492 525 800 - Fax : 33 (0) 492 525 801 e-mail : contact@ard.fr – www.ard.fr

Etablissements de santé

Actualités Produits

GEC

GEC à partir de la version v2.14.x

Dans le cadre de la mise en conformité de la suite GEC (GEC Gestion, GEC Caisse, GEC Kiosk) à la RGPD (Règlement Général sur la Protection des Données), le mécanisme de gestion des mots de passe d'accès a été renforcé.

L'intégration des imprimantes cartes de la gamme « Evolis» avec coupleur de carte à puce intégré est maintenant disponible. Cette fonctionnalité permet l'enrôlement et l'impression (unitaire et par lot) des badges en une seule passe.

Les connecteurs de provisoning et synchronisation ont aussi évolué :

- Connecteur « Texte » : élargissement des données collectées (jours mangés, email, etc.)
- Connecteur ARD Access : prise en compte des actions d'ajout, modification, suppression de porteurs avec catégorie d'accès ou catégorie restauration, prise en compte des photos et identifiant de badge selon formatage ARD ou partenaire.

Mais les évolutions majeures concernent GEC En Ligne :

- Ergonomie repensée pour s'adapter à l'usage des services en ligne depuis un smartphone, une tablette ou un ordinateur (mode Responsive).
- Nouvelles fonctionnalités : consultation de l'historique des consommations, création de l'espace d'administration (permet l'affichage d'un message personnalisé en page d'accueil de GEC En ligne, l'affichage d'un menu de restauration, la gestion des comptes en ligne), paramétrage des périodes de suspension du module de rechargement de compte ou de réservation en ligne, réinitialisation de mot de passe en ligne.
- Intégration dans divers environnements Numériques de Travail (ENT).

Côté matériel

Fin de commercialisation des capots pour chariot de distributeur de plateaux, remplacés par une housse de protection.

ARD s'agrandit…

Cote commercial, Charles Legrain rejoint la force commerciale d'ARD en Ile de France. Charles est à l'origine un spécialiste des solutions de sureté.

Justine Pallu vient également d'être recrutée en tant qu'assistante commerciale pour le secteur EST.

Justine Wandler et Solène Mezmez nous ont rejoint. Elles sont chargées de gérer l'accueil hotline et d'assister la force commerciale SUD.

Côté technique, notre maillage territorial s'enrichit dans l'EST avec le recrutement de Damien Guinet pour le secteur de Valence/Lyon.

Enfin Didier Charpentier, rejoint l'équipe des ingénieurs chargés d'Affaires, il est basé en Ile de France.