Minimieren Sie Ihr Sicherheitsrisiko mit den Lösungen der DN Series™

Diebold Nixdorf

DieboldNixdorf.com

Sicherheit in einer komplexen Welt

Angriffe auf SB-Systeme nehmen zu und verändern sich fortlaufend. Sie verbreiten sich von einer Region zur nächsten und sind sehr unterschiedlich und komplex.

Bei Diebold Nixdorf beobachten und untersuchen wir kontinuierlich neu aufkommende Bedrohungsszenarien bestehend aus Cyber-, Daten und physischen Angriffen, um sie besser zu verstehen und unsere Gegenmaßnahmen immer wieder neu zu justieren.
Die DN Series wirkt den verschiedenen Bedrohungsformen mit branchenführenden, innovativen Lösungen entgegen und reduziert damit das allgemeine Sicherheitsrisiko im Umfeld der SB-Systeme.

Globale Bedrohungsformen

	Physisch	Daten	Cyber
Definition	Alle Betrugs- und Sicherheitsvorfälle die darauf abzielen, physischen Zugang zum Geld im Automaten zu bekommen	Alle Betrugs- und Sicherheitsvorfälle, die darauf abzielen, physischen und/ oder digitalen Zugang zu Kartendaten zu erlangen	Alle Betrugs- und Sicherheitsvorfälle, die darauf abzielen, physischen und/ oder digitalen Zugang zu Systemen/ Kommunikations-Daten und Bargeld im Geldautomaten zu erlangen.
Angriffs-Typen	GAA Sprengungen GAA Aufbruch GAA Diebstahl Bohren, in Brand setzen, schneiden Cash Trapping Transaction Reversal Fraud	Skimming Shimming Software Skimming Abhörangriffe auf Daten Card Trapping Shoulder Surfing	Host Manipulation Jackpotting (Schadsoftware) Jackpotting (Blackbox) Weitere Schadsoftware (Ransomware) Verletzung der Cloud/Host Datensicherheit

Seit mehr als 160 Jahren schützt Diebold Nixdorf Menschen, Daten und Vermögenswerte.
Wir wissen, dass es nicht die EINE Lösung für die Sicherheit gibt. Deshalb bieten wir mit der DN Series vielfältige, intelligente und zielgerichtete Sicherheitslösungen, die Ihre Risiken mindern und Ihre Anforderungen mit den Erwartungen Ihrer Kunden an den Datenschutz in Einklang bringen.

Die DN Series wurde mit einem Basis-Sicherheitsstandard entwickelt, der direkt ab Werk geliefert wird und individuell um zusätzliche Schutzmaßnahmen ergänzt werden kann, um damit Ihren risikobasierten Strategien und unterschiedlichen Einsatzumgebungen gerecht zu werden.

Physische Attacken

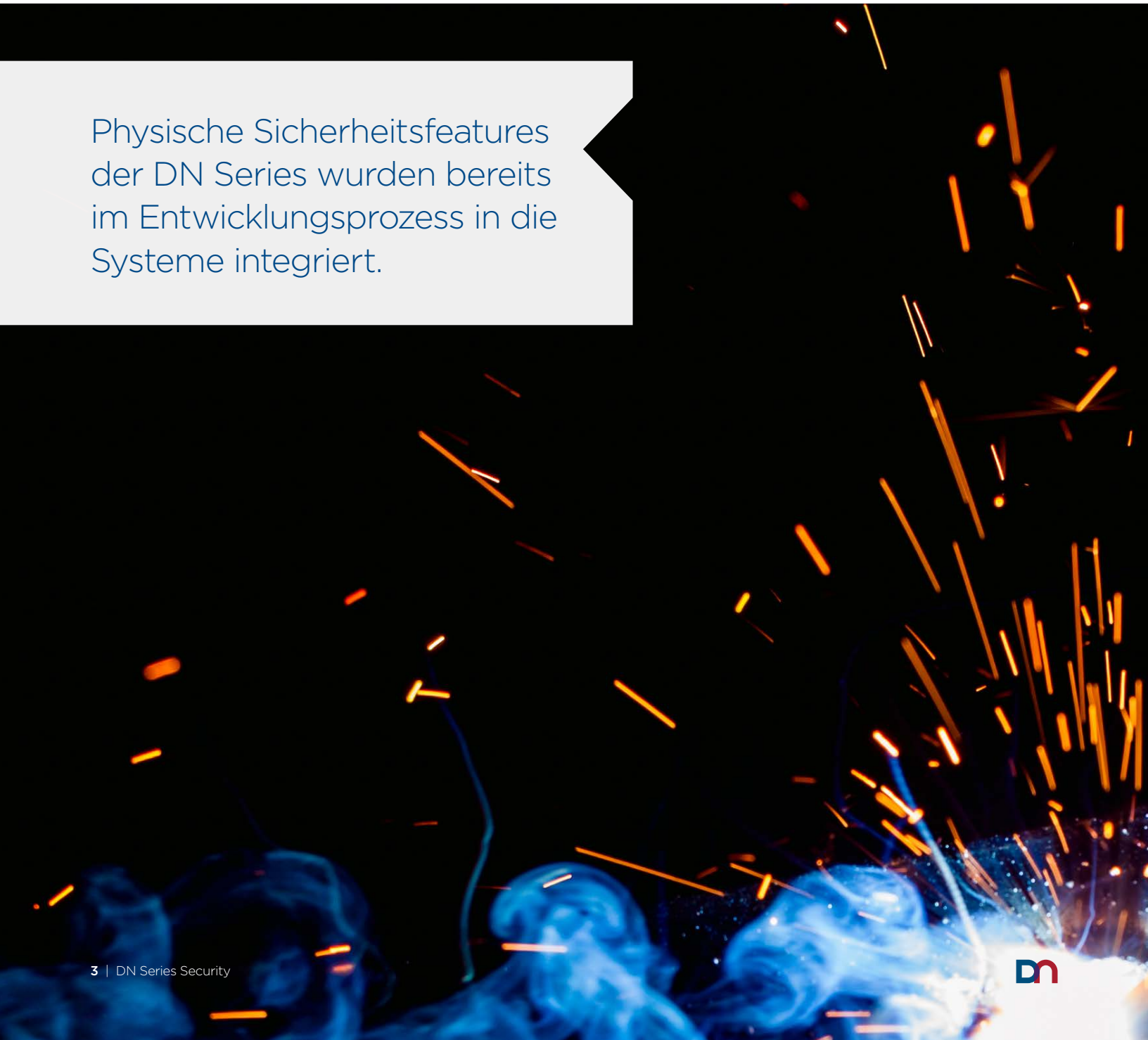
WAS SIE BEDEUTEN

Die Mehrzahl der physischen Angriffe besteht aus Sprengstoff-Attacken, die den Geldautomaten ganz oder teilweise zerstören und damit unbrauchbar machen. Kriminelle können sich so Zugang zu dem darin befindlichen Bargeld verschaffen.

WELCHE FOLGEN SIE HABEN

Sprengangriffe können äußerst kostspielig sein, da die Banken nicht nur den zerstörten Geldautomaten ersetzen müssen, sondern auch mit zusätzlichen Schäden zu rechnen ist, die möglicherweise in der Umgebung entstanden sind. Physische Angriffe bringen aufgrund ihres gewalttätigen Charakters auch andere in Gefahr.

Physische Sicherheitsfeatures der DN Series wurden bereits im Entwicklungsprozess in die Systeme integriert.



Die DN Series macht den Unterschied:

SICHERES TRESOR- UND NOTENWEGE-DESIGN
Die Lage der Notenwege mit mehr Abstand zum Geldausgabefach schützt vor Noten-Phishing und Sprengangriffen.

ANTI-CASH TRAPPING SENSOREN
Intelligente Sensoren erkennen Manipulationen des Geldeingabe-/-ausgabefaches.

VERSTÄRKUNG DER HARDWARE (CHASSIS AND SAFE ENFORCER)
Chassis Absicherung
Verstärktes Systemchassis und zusätzliche Bedienfeldverriegelungen erschweren Systemzugang.

Tresor Absicherung
Abdeckungen für alle Tresoröffnungen und der Einsatz verstärkter Stahlplatten sorgen für einen zusätzlichen Schutz gegen Aufbruch- und Gasangriffe.

BREITE PALETTE AN TRESOR-SICHERHEITSLEVELN
Vom UL bis zum CEN IV EX GAS Tresor

ERWEITERTE ALARMOPTION
ActivGuard (intelligentes Sicherheitsboard) erkennt und meldet mittels bis zu 12 verschiedener Sensoren aktuelle Ereignisse vom Geldautomaten.

TINTEN-KASSETTEN
Tinte entwertet alles Bargeld in den Kassetten, sobald Sensoren unbefugte Fremdeinwirkung erkennen.

RECYCLING-MODUL ZUGRIFFSKONTROLLE
Ein zusätzliches Sicherheitsverfahren erlaubt nur autorisierten Mitarbeitern den Zugang zum Recyclingmodul, wenn sich Bargeld im Escrow oder oberen Fach befindet.

Reduzieren Sie die physischen Angriffe. Vielfältige Sicherheitsfunktionen der DN Series machen Ihre SB-Systeme widerstandsfähiger gegen traditionelle Bedrohungen.

Daten Angriffe

WAS SIE BEDEUTEN

Fortschreitende Skimming-Technologien machen es Kriminellen zunehmend leichter, Karteninhaberdaten über eine Elektronik zu stehlen, die sie vorher im Geldautomaten angebracht haben. Sie befinden sich oft im Kartenleser kombiniert mit Kameras, die auf das PIN Pad gerichtet sind, um die PIN des Benutzers auszuspähen. Kriminelle sind mittlerweile in der Lage, einen Skimmer zu erstellen, der so dünn wie ein Blatt Papier ist.

WELCHE FOLGEN SIE HABEN

Skimming ist die größte Bedrohung unter den Daten Angriffen. Skimming- Attacken am Geldautomaten können ein Institut bis zu 300.000 EURO kosten - und dort ist der Markenschaden und der Vertrauensverlust der Kunden gegenüber dem Institut noch nicht mit eingerechnet[1].

Wir haben das fortschrittlichste Anti-Skimming-Portfolio der Branche entwickelt und schützen damit die Daten Ihrer Kunden und den Ruf Ihrer Marke.

Source: [1]Global Fraud and Security Survey 2017, ATMIA

Die DN Series macht den Unterschied:

ANTI-SKIMMING KARTENLESER

Wir bieten ein breites Angebotspaket mit modularen, skalierbaren Lösungen - passend für jede Einsatzumgebung.

Chip Only	Basic	Advanced	Security Pack 1	Security Pack 2	Security Pack 3
Liest ausschließlich Chipkarten. Spezifischen Ländern vorbehalten.	Basis-Schutz ist Standard bei jedem Kartenleser der DN Series.	Basis-Schutz + intelligente Phishing-Abwehr	Basis-Schutz + intelligente Phishing-Abwehr + Multi-Signal Jamming (stören)	Basis-Schutz + intelligente Phishing-Abwehr + Multi-Signal Jamming (stören) + Erkennen von Skimmern	Premium Schutz mit allen Sicherheitsfeatures + Kernverschlüsselung und Scrambling-Technologie

BASIS SICHERHEITS-STANDARDS BEI ALLEN KARTENLESERN

Trusted Device Communication

Verschlüsselte Kommunikation schützt vor Angriffen auf die Daten der USB-Anbindungen und vor unbefugtem Gerätetausch.

Anti-tapping defense

Eine physikalische Barriere schützt vor Angriffen auf die Daten/ Kommunikation der exponierten Elektronik.

Internal space defense

Minimiert den Freiraum im Kartenleser und schützt damit vor flachen (razor-thin) internen Skimmern. Sichert die Spuren 1, 2 und 3 der Kartenhalterdaten.

Erkennen von internen Skimmern

Schützt vor flachen (razor-thin) Skimmern im Kartenleser durch einen Software-Algorithmus, der erkennt, wenn ein Gerät zu lange im Kartenleser verbleibt.

EMV zertifiziert

Jeder Kartenleser ist EMV-fähig. Damit machen wir Ihre Systeme nicht nur zukunftssicher, sondern schützen auch diejenigen, die Chipkarten aus anderen Regionen der Welt besitzen.

VERBESSERTE ERKENNUNGS- UND JAMMING (STÖREN) TECHNOLOGIE

Permanenter Schutz durch Multi-Signal- Störsender Technologie gegen moderne, externe Stereo-Skimmer.

PREMIUM SCHUTZ

Das Security Pack 3 sorgt für höchste Datensicherheit und weltweit größtmöglichen Schutz vor Skimming-Angriffen.

EPP V8 MIT PIN PAD SICHTSCHUTZ

Aktuellste (PCI PTS V5) Version, schützt die PINs der Benutzer mit den neuesten Sicherheitsstandards. Remote Key Loading Funktionalität: Signatur SHA-256 / Zertifikate SHA-256 opt.TR-34 (International); NAC2 (F), OPT gem. DK (D).

ALTERNATIVE AUTHENTIFIZIERUNG

Mobil, NFC, Biometrie. Der Einsatz von NFC-Technologie oder biometrischen Fingerprint-Lesegeräten eliminiert Skimming-Attacken vollständig.

OVERALL DESIGN

Sicheres Transaktionserlebnis - Encrypted Pin Pad mit Sichschutz, beleuchteter Sichtschutz an den Seiten , Sicherheitsspiegel etc.

Lassen Sie nicht zu, dass ein Skimmer oder Daten-Angriff Ihre Systeme gefährdet. Die DN Series bietet weltweit führenden Schutz vor Betrug, so dass sich Ihre Kunden sicherer fühlen können.

Cyber Attacken

WAS SIE BEDEUTEN

Durch Cyber-Angriffe versuchen Kriminelle Zugang zu Bargeld, Kundendaten oder beidem zu erlangen. Rund um den Globus gibt es Jackpotting-Angriffe, bei denen Schadsoftware injiziert oder über Blackbox-Angriffe die Geldautomaten-Software manipuliert wird, um illegale Befehle auszuführen.

WELCHE FOLGEN SIE HABEN

Die Anzahl der Cyber-Angriffe ist 2016–2018[2] um 83% gestiegen -und machen den größten Anstieg von allen Kategorien aus.

Die DN Series bietet eine Vielzahl intelligenter Standardlösungen, um Cyber-Angriffe abzuwehren.

Source: DN proprietary research

Die DN Series macht den Unterschied:

ANOMALY DETECTION ENGINE (ADE)

Eine integrierte intelligente Software, die anomales Verhalten am Geldautomaten identifiziert, protokolliert und korreliert. Beispiele hierfür sind:

- Eine übermäßige Anzahl von Bargeldabhebungen mit derselben Karte signalisiert einen Jackpotting-Angriff
- Wenn eine Bankkarte zu keinem Zeitpunkt aus dem Kartenleser herausgenommen wird, signalisiert dies eine mögliche Card Trapping Attacke.

CORE COMPUTING SECURITY

Trusted Device Communication (TDC)

- Software, die die USB-Kommunikation zwischen dem PC und sicherheitsrelevanten Modulen verschlüsselt. TDC stellt sicher, dass nur autorisierte DN Module und -Komponenten in den Geldautomaten integriert werden können.
- TDC ist standardmäßig in jedem Modell der DN Series enthalten und schützt die kritischen Module.
- Trusted Platform Module (TPM) dient als Sicherheitsgrundlage und stellt sicher, dass nur autorisierte DN Module miteinander kommunizieren.

Basic Endpoint Security (BES)

- Cyber-Sicherheitssoftware, die einen Basisschutz vor Cyber-Angriffen bietet. Der Schutz umfasst USB-Whitelisting, Basishärtung des Betriebssystems und eine Windows-Firewall. Die Software kann direkt im Werk oder vor Ort hochgeladen werden - Plug-and-Play.

APPLICATION LAYER SECURITY

Vynamic Security Suite

- Eine umfassende, innovative und flexible Sicherheits-Software Suite, die auf die Geldautomaten-Umgebung ausgerichtet ist und von DN entwickelt wurde. Die einzelnen Lösungen sind skalierbar und können angelehnt an die individuellen Sicherheitsanforderungen auch gebündelt werden. Sie bieten beispielsweise Schutz vor unbefugtem Systemzugriff, Jackpotting-Angriffen oder der Einschleusung von Schadsoftware.
  - Festplattenverschlüsselung
  - Intrusion Protection (Abwehr von Angriffen)
  - Zugriffsschutz

Vynamic View Security Manager

- In Verbindung mit der Vynamic Security Suite agiert der Vynamic Security Manager als die zentrale Instanz für das Empfangen von sicherheitsrelevanten Ereignissen, Weiterleitung von Alarmen sowie das Aktivieren neuer Sicherheitsregeln.

TRUSTED APPLICATION SOFTWARE

Abgesicherte Pin Eingabe und Verarbeitung mit PCI PA – DSS Version 3.2; erfordert TLS 1.2 +, um Man-in-the-Middle-Angriffen vorzubeugen.

AUTHENTIC DN PLATFORM SOFTWARE

Signatur-Validierung über Vynamic Security Intrusion Protection.

CRYPTA STICK

Autorisierter Service-Token (USB), der in den Geldautomaten eingesteckt wird und sicher stellt, dass nur autorisiertes Personal auf interne Software und Funktionen zugreifen und diese nutzen kann.

Die Anzahl der Cyber-Angriffe ist weltweit gestiegen - mit der DN Series bieten wir Ihnen mehr Schutz gegen diese Bedrohungen.

Take ACTion

Unser ACTions-basierter Sicherheitsansatz bietet Ihnen drei wichtige Eckpfeiler zur Abwehr von Angriffen.

Analysieren | **Kommunizieren** | **Verfolgen**

NUTZEN SIE UNSER GLOBAL SECURITY PORTAL

Informieren Sie sich regelmäßig über die neuesten Bedrohungen, die Ihre Region betreffen. Registrieren Sie sich auf unserem ACT-Portal, damit Sie den Überblick darüber haben, wie Sie Angriffe auf Ihre Geldautomaten vermeiden können.

UNTERSTÜTZT WERDEN SIE VON DEN DN ALLCONNECT MANAGED SECURITY SERVICES℠

Sie arbeiten mit Experten zusammen, die Sie individuell unterstützen. Unsere Managed Security Services verfolgen einen umfassenden Ansatz zur Sicherung Ihrer Daten, Kanäle und Systeme, während Sie sich auf wichtigere Dinge konzentrieren können.

PROFITIEREN SIE VOM INNOVATIVEN DESIGN DER DN SERIES

Die DN Series wurde für eine moderne, vernetzte Welt entwickelt. Erfahren Sie mehr darüber, wie die DN Series physische und digitale Kanäle miteinander verbindet, Transaktionen automatisiert und es Ihnen ermöglicht, Ihren Kunden mehr zu bieten - und das alles in einer sicheren, konformen Umgebung.

NUTZEN SIE DIE VORTEILE UNSERER GEBÜNDELTEN SICHERHEITSLÖSUNGEN

Profitieren Sie vom Mehrwert der DN Series. Unsere "MORE SECURE"-Lösungspakete bieten Ihnen die Flexibilität, die Ihren strategischen Anforderungen entspricht. Sprechen Sie mit uns und informieren Sie sich über Pakete und Optionen, die Ihren Wünschen entsprechen.

Visit DieboldNixdorf.com/DNseries.

Diebold Nixdorf

DieboldNixdorf.com