IT-Sicherheit für Energieversorgungsunternehmen

Autor(en): **Eisen, Goswin**

Objekttyp: **Article**

Zeitschrift: **Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses**

Band (Jahr): **91 (2000)**

Heft 7

PDF erstellt am: **13.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-855537

IT-Sicherheit für Energieversorgungsunternehmen

Informationen und Informationssysteme sind für die zunehmend vernetzte Elektrizitätswirtschaft von existenzieller Bedeutung. Ihre Beeinträchtigung kann für Energieversorger und ihre Kunden existenzbedrohend sein. IT-Sicherheit als ganzheitlicher Ansatz zum Schutz derartiger Systeme und zur Bewahrung von Integrität, Vertraulichkeit und Verfügbarkeit von Systemen und Daten ist von vitaler Bedeutung für die Elektrizitätswirtschaft.

Die Elektrizitätswirtschaft befindet sich in einem radikalen Wandel – die Grenzen der geschlossenen Versorgungsgebiete und andere Monopole fallen, die Neuverteilung der Märkte hat begonnen.

Die Ware Energie muss in Zukunft unter Kosten- und Marktpreisbedingungen produziert, kalkuliert, segmentiert, vermarktet und vertrieben werden. Der Konzentrationsprozess durch Übernahmen oder strategische Kooperationsmodelle ist im Gange, eine Normalisierung des Marktes wird sich erst in den nächsten Jahren heranbilden. Die Reorganisation in Richtung zukunftgerichteter Unternehmensstruktur erfordert ein komplettes Reengineering der Prozesse. Dabei wird der Informationstechnik (IT) in allen Bereichen eine Schlüsselrolle zukommen. Alte, oft eigenentwickelte Softwaresysteme und IT-Infrastrukturen werden den neuen Anforderungen nicht mehr gerecht, sie sind häufig nicht aufeinander abgestimmt, unflexibel und teuer in Wartung und Upgrade.

Neue IT-Konzepte sollen Transparenz und Durchgängigkeit des Material- und Werteflusses über die gesamte Wertschöpfungskette sicherstellen.

Bisherige Inselprozesse von Energieversorgern in den Bereichen Finanzwesen, Anlagebuchhaltung, Materialwirtschaft, Personalwesen, Vertrieb und Projektsteuerung werden durch Standardprozesse ersetzt, wie das Beispiel SAP Utilities (Bild 1) stellvertretend für die Gesamtbranche deutlich macht.

Adresse des Autors
Dr. *Goswin Eisen,* Leiter Competence Center IT-Sicherheit, CSC Ploenzke
D-80335 München
E-Mail geisen@cscploenzke.de

Zunehmende Vernetzung

Wichtigstes IT-Thema für Energieversorger ist neben der Optimierung und Standardisierung der internen Prozesse und der Effizienzsteigerung die Vernetzung mit Kunden, Lieferanten und Partnern.

Das Konzept E-Utilities (E-Commerce) für Energieversorger von CSC Ploenzke beispielsweise bietet Energieversorgern eine Möglichkeit, um auf den liberalisierten Märkten flexibel und erfolgreich agieren zu können.

- Utilities to Client (U2C) ermöglicht es, das vollständige Angebot elektronisch abzuwickeln. In Zukunft wird hierin ein erhebliches Einsparungs- und Servicepotenzial liegen.
- Utilities to Government (U2G) bezeichnet die elektronische Geschäftsbeziehung zwischen Energiewirtschaft und Behörden, z.B. bei Baugenehmigungen oder Anmeldungen
- Utilities to Utilities (U2U) vernetzt und optimiert die Prozesse in den neuen Geschäftsbeziehungen zwischen Erzeugern, Transporteuren und Verteilern und ermöglicht die Bildung neuer Vertriebs- und Anbieter-Allianzen.

IT-Sicherheit – eine umfassende Aufgabe

Weil Energieversorger sich immer stärker auf Netzwerke und Informationssysteme abstützen, um ihre zentralen Prozesse zu unterstützen, wird auch der Schutz und die Verfügbarkeit von IT-Systemen zur immer wichtigeren Aufgabe.

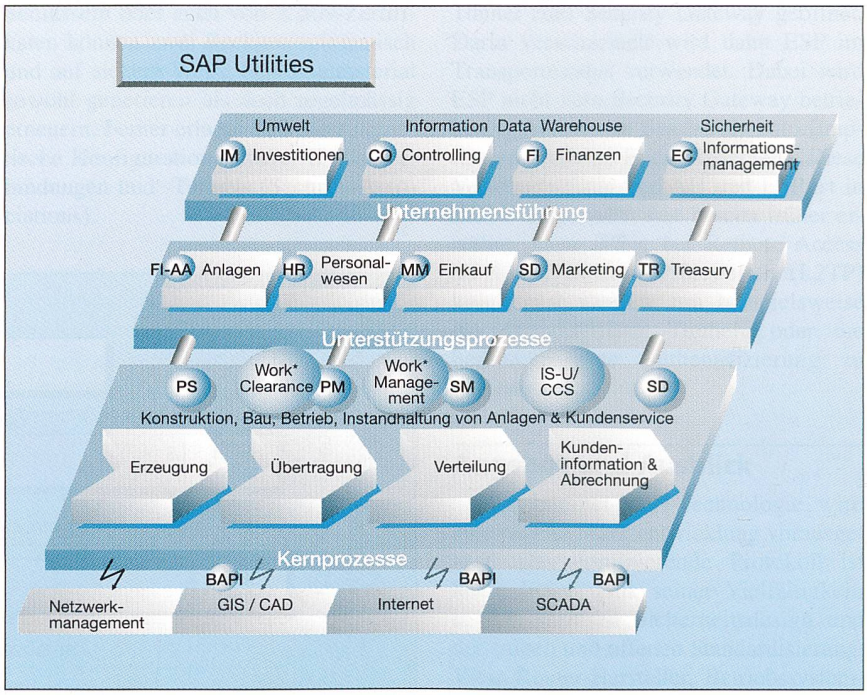

Bild 1 Zusammenwirken von Softwaremodulen in den verschiedenen Bereichen eines Versorgungsunternehmens

Die betriebswirtschaftlichen Abläufe sind komplex und ineinander verflochten. ERP-Lösungen sind in der Lage, diese Strukturen abzubilden und dabei individuelle Aspekte der verschiedenen Unternehmen zu berücksichtigen.

Ein Problem – viele Ebenen

Sicherung verteilter Applikationen
- Sicherheits-Policy und -Modelle, Protection Profiles
- Authentizierungsschemen und Protokolle
- Autorisierungsschemen und Protokolle, Single Sign-on
- Kommunikationssicherheit
- Sicherheit zwischen verschiedenen Standorten
- Sicherheit der Applikationen wie SAP

Sicherheit verteilter Systeme und Netzwerke
- Netzwerk-Sicherheitsarchitektur
- Sicherheit von Middleware (DCOM, Corba, RMI)
- Mobile Security, z.B. WAP
- LAN-Sicherheit
- WAN-Sicherheit
- Hochgeschwindigkeitsnetzwerk-Sicherheit
- Sicherheitsmanagement
- Signalübermittlungssicherheit

Sicherer E-Commerce
- Sichere E-Zahlungen
- Sicherheitsprotokolle
- Formale Analysen
- Public Key Infrastructure
- Digitale Signaturen

Sichere Messgeräte
- Sichere Messgeräte und Erfassung via Handheld
- Sichere Messdatenübermittlung
- Sichere externe Geräte wie Zeiterfassung, Fahrtenschreiber, Chipkarten

Erfüllung von nationalen und internationalen Sicherheitsstandards und Vorschriften
VSE- oder VDEW-Standards:
- BS7799 (UK)
- ISO Security
- IETF (Internet) Security
- OSF/Open Group Security
- IEEE Network Security
- OMG/Cobra Security
- IT SEC/Common Criteria
- Daten- und Persönlichkeitsschutz

Sicherheitsmanagement
- Risk Management, Sicherheitsmanagement
- Sicherheitszertifizierung

Der Bedarf an IT-Sicherheit wächst zurzeit exponentiell. Das grosse Innovationstempo und die zunehmende Vernetzung stellt Elektrizitätsversorger vor eine ganze Reihe von IT-Sicherheitsproblemen:

- Wachstum und horizontale und vertikale Zusammenschlüsse von Elektrizitätsversorgern mit unterschiedlichen Systemen und Sicherheitskulturen*
- Einsatz mobiler Computer
- Einsatz mobiler Messgeräte, Datenübermittlung und Einspeisung in Netzwerke*
- Digitale Messgeräte mit Datenübermittlung via Modem*
- Flexible Zusammenarbeit mit Partnern und Lieferanten
- Einsatz von Sub-Unternehmern
- Virtuelle Netzwerke
- E-Commerce und Strombörsen
- Freie Wahl des Energieversorgers durch Kunden*
- Verschärfte gesetzliche Regelungen
- Erfüllung von nationalen und internationalen Sicherheitsstandards und Vorschriften*

* EVU-spezifisch

Für die Elektrizitätsversorger werden international akzeptierte, sichere IT-Lösungen für die Erfassung, Übertragung und den Austausch von Betriebs-, Verrechnungs- und Managementdaten von ebenso grosser Bedeutung sein wie eine stabile Energieversorgung. Sichere Informationstechniksysteme sind mithin eine Voraussetzung für den liberalisierten Energiemarkt.

Vielschichtige IT-Strukturen

In aller Regel sind die IT-Strukturen und Netzwerke von Elektrizitätsversorgern ausgesprochen vielschichtig. Sie umfassen komplexe und grosse Computersysteme und Datenspeicher, interne und externe EDV-Netze, Anschluss an öffentliche und private Fernmeldesysteme, Funkkommunikation, mobile Datenerfassung und -übermittlung, Vernetzung und Geschäftsabwicklung via Internet. In vielen Bereichen müssen Systemdienstleistungen und Daten 365 Tage im Jahr und rund um die Uhr zur Verfügung stehen.

Auch die Elektrizitätszähler sind heute Bestandteil der Informationssysteme, wobei die Messdatenerfassung über Vor-Ort-Ablesung und Eingabe in Handheld-Terminals oder bei modernen Lastprofilzählern über Fernablesung via Modems erfolgt. Hier sind verschiedene Standardisierungsbemühungen auf nationaler und internationaler Ebene im Gange (z.B. nach DLSM/Cosem: Device Language Message Specification/Companion Specification for Energy Metering in Deutschland).

Das sind die wichtigsten Sicherheitsrisiken für die IT von Elektrizitätsunternehmen:
- Naturkatastrophen
- Brand und Brandlöschung
- Baumängel
- Physische Beschädigung oder Sabotage von Systemen, Daten und Netzwerken
- Elektrizitätsversorgung der IT wird unterbrochen
- Computerviren können Systeme lahm legen und Daten zerstören
- Fehlerhafte oder manipulierte Software
- Manipulation von Daten, auch von Messdaten
- Abstreiten von erfolgten Datenübermittlungen
- Fälschung von Kunden- oder Partnertransaktionen
- Bekannt werden von vertraulichen Kunden- oder Mitarbeiterinformationen
- Sabotage durch externe Hacker oder interne Mitarbeiter

- Unerwünschte Rekonfiguration von Systemen, Missbrauch
- Denial of Service: Internet-basierte Dienstleistungen werden durch Massenangriffe verunmöglicht, Systeme blockiert
- Abhören der Kommunikation

Nichttechnische Aspekte

Auf den ersten Blick erscheint IT-Sicherheit ein klar umgrenztes technisches Thema zu sein. Und tatsächlich gehören die Absicherung der IT-Infrastrukturen und ihrer einzelnen Komponenten durch technische Konzepte und die Auswahl und Implementierung der geeigneten Tools zu den wichtigsten Aufgaben auf diesem Gebiet. Mit der Installation von Anti-Viren-Software und einem adäquaten Passwortschutz ist es allerdings nicht getan. IT-Sicherheit umfasst weit mehr. Sie erfordert heute Vertrautheit mit Technologien wie Eindringungsentdeckung, Firewall-Technologien, Biometrie, Audit Trails (Nachverfolgung des Informationsflusses) und Authentifizierung, Verschlüsselungen und digitalen Signaturen.

Es genügt nicht, die höchstentwickelten Technologien einzusetzen. IT-Sicherheit erfordert die ganzheitliche Betrachtung der Information, die Beurteilung der Risiken und Gefahren und die Umsetzung geeigneter Massnahmen, um Risiken im Griff zu haben.

CSC Ploenzke gehört zu den grossen IT-Beratungsunternehmen im deutschsprachigen Raum. Speziell in der Elektrizitätswirtschaft war das Unternehmen, eine Tochterfirma der Computer Science Corporation (CSC), für die Installation von rund 200 Enterprise-Ressource-Planning(ERP)-Lösungen verantwortlich. In der Schweiz wurden Projekte für die Elektrizitätswerke Zürich und Bern (EWZ und EWB), Elektra Birseck EBM und die CKW Luzern realisiert. Daneben entwickelte die Firma das Grundschutz-Tool des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Kontakt: Sandra Voeller, Leiterin des Geschäftsbereichs Energieversorger, CSC Ploenzke (Schweiz) AG, Telefon 01 307 22 22.

Um Sicherheit zu erreichen und zu garantieren, ist eine Erarbeitung und Umsetzung von Sicherheitsstrategien und Rahmenkonzepten erforderlich, abgestimmt auf die Bedürfnisse der Organisation. Dazu müssen die Auswirkungen auf die IT-Organisation bewertet, die Rollen und Verantwortlichkeiten genau definiert und in der Organisation etabliert werden.

IT-Sicherheitskonzepte müssen Defizite erkennen, vorhandene (und zukünftige) Risiken und Gefährdungen identifizieren und anforderungsgerecht Massnahmen und Regelungen definieren. Wesentlich für den Erfolg ist neben der ganzheitlichen Betrachtungsweise die konsequente und komplette Umsetzung.

Sicherheitskonzepte müssen immer in Rechnung stellen, dass die grössten Fehlerquellen und Sicherheitsrisiken im menschlichen Verhalten liegen, vom unabsichtlichen Fehler bis hin zum bewussten kriminellen Handeln. Dies kann interne und externe Mitarbeiter, Kunden und Partner gleichermassen betreffen. Sicherheitskonzepte und Technologien können dies weitgehend verhindern, indem sie geeignete Massnahmen vorsehen, klare Prozesse definieren und zur Sensibilisierung von Organisationen und Mitarbeitern beitragen.

Komplexe Netze erfordern umfassenden Schutz

Die Lösungen müssen möglichst alle Anforderungen aus folgenden Bereichen vollständig berücksichtigen:

- Umfassende Betrachtung der gesamten IT-Sicherheitsstrategie und Infrastruktur
- Überprüfung bestehender Prozesse und Lösungen
- Ausarbeitung einer unternehmensweiten Sicherheitspolitik
- Schutz von Endsystemen
- Schutz von verteilten Applikationen
- Erkennung und Abwehr von Angriffen im Netzwerk
- Kontrolle und Filterung des Datenaustausches und des Netzverkehrs
- Beweisbare Identifikation von Kommunikationspartnern
- Sicherstellung von Integrität, Verfügbarkeit unternehmenseigener und sensibler Daten
- Aufklärung, Sensibilisierung und Schulung der Mitarbeiter

Betrachtet man den IT-Schutz von Unternehmensdaten, so sind neben Zugangs- und Zugriffsschutz auch die Integrität und Verfügbarkeit der Daten sicherzustellen und dauerhaft zu gewährleisten.

Die Verfügbarkeit und Funktionsfähigkeit von Netz, Systemen, Applikationen und Daten verlangt nach konsequenten Lösungen im Bereich Archivierung, Datensicherung, Ausfallsicherheit, Katastrophenvorsorge und «Desaster Recovery».

Auf der Applikationsebene steht insbesondere der Schutz verteilter Standardlösungen (Baan, SAP oder Data Warehousing) und des entsprechenden Umfelds im Vordergrund. Weil vielfach die Benutzer von internen Anwendungssystemen im Fakturierungs- oder Marketing-

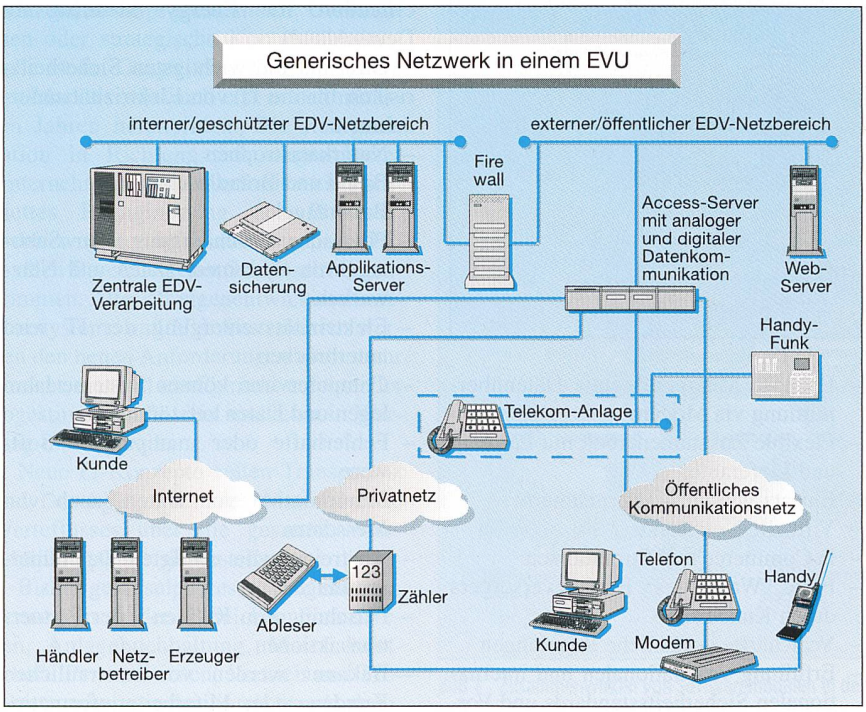

Bild 2 Generisches Netzwerk

Die Netzwerke von EVU haben sich geöffnet. Die Systeme kommunizieren intern und extern, dadurch vergrössern sich die Risiken. Sicherheitskonzepte müssen dies berücksichtigen.

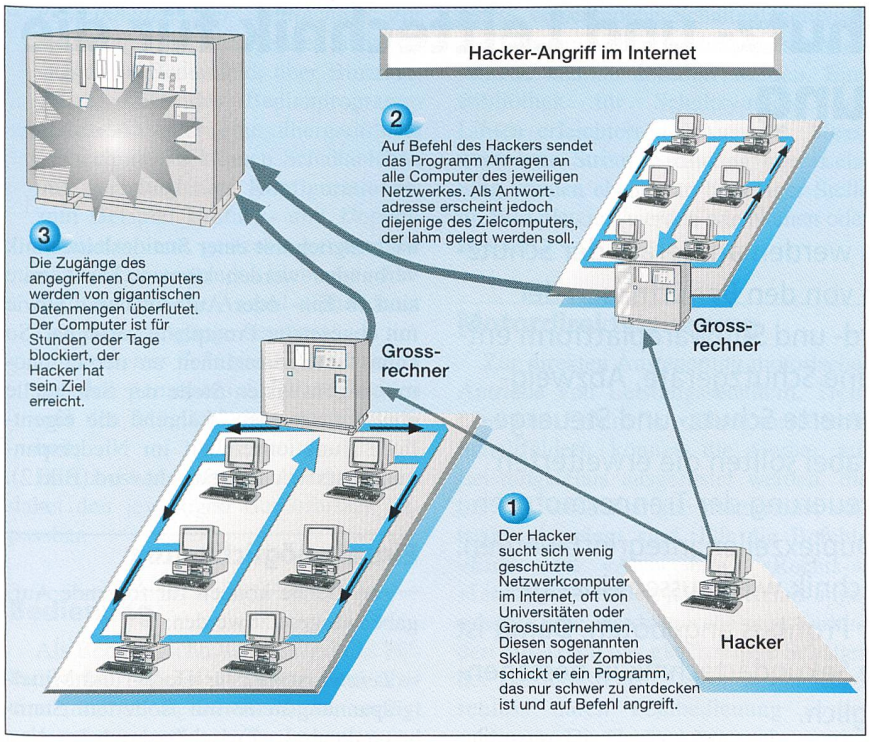

Bild 3 «Denial of Service»-Angriff

bereich über weitgehend ungesicherte Kanäle kommunizieren, müssen Applikationen, Zugriff und Schnittstellen abgesichert werden.

Im Bereich Internet und E-Commerce haben spektakuläre Ereignisse dem Thema Sicherheit zu besonderer Aktualität verholfen. Besonders die jüngsten «Denial of Service»-Attacken, z.B. bei Yahoo, haben gezeigt, wie wichtig das Thema Sicherheit geworden ist. Im Weissen Haus fand dazu eine eigentliche Krisensitzung statt – einberufen und geleitet von US-Präsident Bill Clinton höchstpersönlich! Ausserdem wurde von der amerikanischen Regierung eine Untersuchung in Auftrag gegeben, die die Verletzbarkeit bundesstaatlicher Computersysteme durch «Denial of Service»-Angriffe ermitteln soll. Ein Beispiel, dem viele private Unternehmen in Amerika folgen werden.

Die Datenintegrität im Bereich der Ablese- und Verbrauchsdaten – Rohdatenerfassung, Übermittlung, Aufbereitung und Umwandlung zur Grundlage für die Fakturierung für verschiedene Kundengruppen – erfordert neue technische und organisatorische Verfahren, wobei Datenschutz und Vertraulichkeit von grösster Bedeutung sind.

Für den elektronischen Handel muss die Sicherheit nach international akzeptierten Standards garantiert werden, beispielsweise Edifact oder Secure Electronic Transaction (SET). Für Netzkunden, welche sich nicht am elektronischen Handel beteiligen, müssen Messdaten über andere, ebenfalls abgesicherte Datenschnittstellen zur Verfügung gestellt werden.

IT-Sicherheit ist kein Zufallsprodukt

Sicherheit ist zu wichtig, um auf Grund von Ad-hoc-Entscheidungen oder als (Schreck)-Reaktion auf Ereignisse geregelt zu werden. Die IT-Sicherheit vollzieht sich als zyklischer Prozess: Neue unternehmerische Aufgaben, neue Technologien und neue Mitarbeiter bringen neue Risiken und erfordern daher die kontinuierliche Überprüfung der bestehenden Sicherheitsstruktur.

Permanentes IT-Sicherheitsmanagement ist deshalb eine Aufgabe, die umfassend ist und auf die Stufe der obersten Unternehmensleitung gehört. Von entscheidender Bedeutung ist eine Verankerung in der Unternehmenskultur. Fehlendes Sicherheitsbewusstsein und Kenntnisse der Mitarbeitenden führen zu Fahrlässigkeit, Unverständnis und zu Risiken.

Dabei darf Sicherheitsmanagement nie zum Selbstzweck werden: Weil Sicherheit immer mit Aufwand, Kosten und gewissen Einschränkungen verbunden ist, müssen Massnahmen und Technologien auf einem konkreten Bedarf beruhen. So werden nicht nur die Unternehmensressourcen, sondern auch die IT-Investitionen optimiert.

Sicherheitsmanagement umfasst:

- Aufbau des IT-Sicherheitsmanagement-Teams
- Ausarbeitung der Sicherheitspolitik in Übereinstimmung mit übergeordneten Vorgaben
- Erstellung, Überprüfung und Weiterentwicklung von Sicherheitskonzepten
- Sicherheitsbedarfsanalyse, Bedrohungs- und Risikoanalyse, Assessment der bestehenden technischen und organisatorischen Vorkehrungen im Umfeld der IT-Systeme
- Organisatorische und technische Massnahmen in Abstimmung mit der IT-Strategie
- Sensibilisierung und Schulung der internen und zunehmend auch externen Mitarbeiter
- Überwachung und Assessment der Akzeptanz und Wirksamkeit getroffener Massnahmen, von Technologien und Prozessen
- Konsequente Weiterentwicklung von Sicherheitsmassnahmen und Lösungen.

Alle Sicherheitsfragen sollten in einem professionellen Sicherheitsmanagement-Team bearbeitet werden, das den gesamten Kreislauf kontrolliert und in Absprache mit den Unternehmensbereichen als interner Servicebereich zentraler Ansprechpartner für alle Sicherheitsfragen ist. In vielen Fällen sollte die Hilfe von externen Experten erwogen werden.

La sécurité informatique dans les entreprises de production d'énergie

Dans l'économie de plus en plus interconnectée de l'électricité, l'information et les systèmes d'information sont d'une importance vitale. Toute entrave au fonctionnement peut menacer l'existence même des fournisseurs d'énergie et celle de leurs clients. La sécurité informatique revêt donc une importance cruciale en tant qu'approche intégrale en vue de la protection de tels systèmes et du maintien de l'intégrité, de la confidentialité et de la disponibilité des systèmes et données dans l'économie électrique.