

Die unbekannte Gefahr



Gefährdung kritischer Infrastrukturen durch elektromagnetische Sabotage

Mit physischen Schutzmaßnahmen, Zutrittskontrolle, Videoüberwachung und einer Vielzahl weiterer Maßnahmen kann ein hoher Sicherheitsstandard für kritische Infrastruktur erreicht werden. Unbeachtet blieben bisher aber oft Szenarien, die sich elektromagnetischer Energie bedienen, um ihr Ziel anzugreifen. Man könnte von „Vorsätzlicher Elektromagnetischer Beeinflussung“ sprechen, englisch „Intentional EMI“. Unter diesem Oberbegriff versammeln sich verschiedene elektromagnetische Phänomene, die sich in Ursache, Ausbreitungsverhalten, Zeitverlauf und Amplitude unterscheiden. ■ Hans Wolfspurger



Rechenzentren, Kraftwerke, leittechnische Anlagen der Energie- und Wasserversorgung, Verkehrsleitsysteme, Knoten von Daten- und Telekommunikationsnetzen, strategisch bedeutsame Produktionsanlagen – all diese Einrichtungen werden oft unter dem Oberbegriff „kritische Infrastrukturen“ zusammengefasst. Eine Störung oder gar der komplette Ausfall einer dieser Infrastrukturen führt zu Schäden gewaltigen Ausmaßes: Zu den unmittelbaren finanziellen Folgen kommen oft volkswirtschaftliche Schäden, die sich kaum beziffern lassen. Kein Wunder also, dass derartige Anlagen mit hohem Aufwand vor äußeren Einwirkungen geschützt werden: Neben dem Schutz vor Elementarschäden wie Wasser oder Brand spielt hier der Schutz

vor vorsätzlicher (Zer-) Störung durch Vandalismus oder Sabotage eine wichtige Rolle. Eine neue Gefahr sind elektromagnetische Angriffe.

Nuclear ElectroMagnetic Pulse, NEMP

Die erste Konfrontation mit dieser Problematik fand nach dem zweiten Weltkrieg statt. Man erkannte, dass bei der Detonation von Kernwaffen eine elektromagnetische Stosswelle mit einer Anstiegszeit von etwa vier Nanosekunden ausgelöst wird. Diese kurze Anstiegszeit sorgt dafür, dass die üblichen Blitzschutzsysteme meist nicht ansprechen. Auch an eine Schirmung werden wesentlich höhere Anforderungen gestellt. Diese Gefährdung ist seit langem bekannt und Bestandteil der Szenarien des „Kalten Kriegs“. In folge dessen wurde militärisches Gerät gegen diese Bedrohung gehärtet und mit entsprechenden Prüfeinrichtungen entsprechend getestet. Ziviles Gerät besitzt im Allgemeinen keinen NEMP-Schutz.

Besonders heftig sind die elektromagnetischen Auswirkungen, wenn eine Kernwaffe in der Atmosphäre (Endo-

NEMP) oder im Weltraum (Exo-NEMP) gezündet wird. Dies wurde erstmals 1962 deutlich, als ein atmosphärischer Atomwaffentest über dem Pazifik im Umkreis von 1200 Kilometern elektronische Geräte lahm legte. Diese Atomdetonationen in großer Höhe zum Zwecke der elektromagnetischen (Zer-)Störung werden auch als HEMP (High Altitude ElectroMagnetic Pulse) bezeichnet.

Derartige Szenarien wurden mit dem Ende des kalten Kriegs vorerst zu den Akten gelegt, bekommen jetzt aber wieder neue Aktualität: Insbesondere in den USA fürchtet man, dass „Schurkenstaaten“ oder terroristische Organisationen in absehbarer Zeit in der Lage sein werden, kleine Atomsprengköpfe zu bauen, die lediglich zum Zweck einer HEMP-Erzeugung in der Atmosphäre gezündet werden. Geeignete Trägerraketen sind bereits im Besitz dieser Länder. Ein derartiger Angriff hätte keine unmittelbare Auswirkung auf die Gesundheit oder gar das Leben von Menschen – allerdings könnte er mit sehr überschaubarem Aufwand in einer großen Fläche riesige materielle Schäden anrichten. Auch wenn dieses Szenario unrealistisch

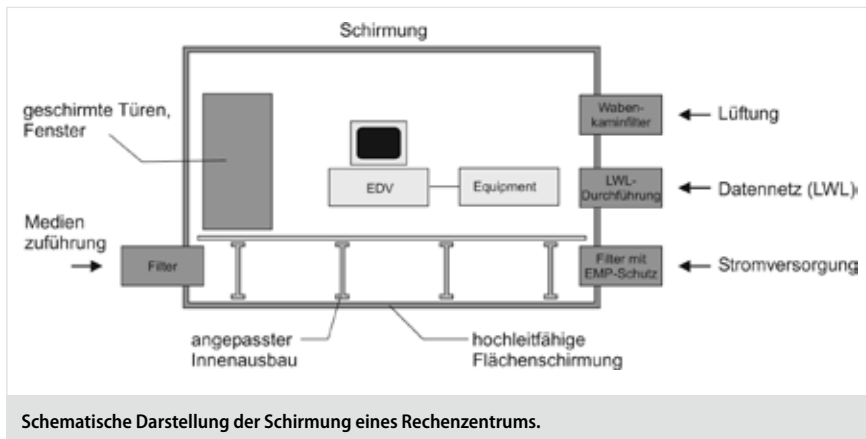
AUTOR

Dr. Hans Wolfspurger
ist Leiter der Technik bei Emscreen
in Taufkirchen

T +49/89/614171-36

F +49/89/614171-71

hwolfspurger@emscreen.de



scheint – bei der Planung zukunftsweisender Projekte wird es bereits berücksichtigt. Der neue Europäische Druckwasserreaktor (derzeit in Finnland im Bau) wird eine HEMP-Schirmung besitzen.

High Power Microwave (HPM)

Handfester ist die Bedrohung durch High-Power-Microwave-(HPM)-Waffen. Die Entwicklung von Impulsgeneratoren ist kein Hexenwerk, sondern eine häufige Aufgabenstellung, für die das Grundwissen an den Universitäten gelehrt wird. In naher Zukunft dürfte sich auch die terroristische Szene derartiger Generatoren bedienen, um Sabotage zu betreiben. Das Prinzip einer derartigen Waffe: Geladene Energiespeicher (z.B. Kondensatoren) werden über schnelle Schalter in extrem kurzer Zeit entladen. Dadurch treten sehr hohe Leistungen (im Tera-Watt-Bereich) auf. Der erzeugte Impuls wird über eine Antenne als elektromagnetische Welle in den freien Raum abgestrahlt.

Elektronische Systeme sind bei Frequenzen im hohen MHz- und im GHz-Bereich besonders verwundbar. Dies machen sich HPM-Waffen zu nutze. Insbesondere Ultra-Wide-Band- (UWB) Generatoren mit Anstiegszeiten < 1 ns strahlen ihre Energie in den Frequenzbereich zwischen 100 MHz und 1 GHz ab, genau in dem Bereich, in dem die meisten elektronischen Geräte besonders empfindlich sind. Zu den HPM-Waffen werden aber auch Generatoren gezählt, die hochenergetische Störungen mit sinusförmigem Zeitverlauf, meist gepulst und gedämpft ausschwingend, erzeugen.

Auch mit einfachen Mitteln lassen sich Schäden anrichten: Der Umbau eines Mikrowellenherdes zum HPM-Generator ist einfach möglich. So lässt sich ein Strahler mit einer Leistung von 1000 W bei einer Frequenz von 2,455 GHz herstellen. Oft

befinden sich Rechnerräume in unmittelbarer Nähe von öffentlich zugänglichem Gelände, getrennt nur durch eine Wand – mit einem PKW kann der Generator so bis auf wenige Meter unentdeckt ans Ziel gebracht werden. Drahtlosanwendungen halten auch im industriellen Umfeld immer mehr Einzug. Die hohe Dichte von Geräten macht oft schon eine standortinterne Planung der Frequenznutzung erforderlich. Insbesondere flexible Produktionsanlagen bedienen sich drahtloser Verbindungen (WLAN, Bluetooth etc.). Mit einfachstem, frei erhältlichem Equipment, wie es unter anderem von Funkamateuren verwendet wird, lassen sich diese Wireless-Anwendungen, wenn auch „nur“ reversibel, stören. Die Auswirkungen, insbesondere bei unregelmäßigem Auftreten, können enorm sein, denn ein kausaler Zusammenhang zwischen Angriff und Schaden ist oft nicht feststellbar und praktisch nie nachweisbar.

Schutz gegen Angriffe

Die Leistungsfähigkeit der beschriebenen Störquellen ist weitgehend unbestimmt. Professionell entwickelte HPM-Generatoren, die im Kfz transportiert werden können, erzeugen elektrische Feldstärken von rund 300 kV/m in einem Meter Abstand. Selbstgebastelte Quellen sind weniger leistungsfähig, aber die Störfestigkeit von herkömmlichem elektronischem Gerät ist um Größenordnungen geringer (Faktor etwa 1 zu 30 000). Für die Prüfung der Störfestigkeit gegen EMP-Beaufschlagung existieren zwar zivile Normen (DIN-EN 61000-4-23, DIN-EN 61000-4-24), es sind aber noch keine verbindlichen Prüfschärfgrade für die Produkte vorgegeben.

Der Aufwand, der zum Schutz vor elektromagnetischer Sabotage betrieben werden muss, hängt im Wesentlichen vom zugrunde gelegten Angriffsszenario ab.

Mit einer Zunahme der Bedrohung in naher Zukunft ist allerdings zu rechnen. Bei der Planung kritischer Infrastrukturen erscheint es fahrlässig, sich mit der Problematik nicht zumindest zu beschäftigen.

Der Schaffung eines ausreichenden Abstandes zwischen unkontrolliert zugänglichem Bereich und der zu schützenden Anlage ist sicher eine einfache Möglichkeit, um eine Gefährdung zu reduzieren. Die Feldstärke (im Fernfeld einer Quelle) nimmt mit dem Faktor $1/r$ ab, das heißt, eine Verdopplung des Abstands halbiert die auftretende Feldstärke. Oft ist dies jedoch nicht ausreichend beziehungsweise eine ausreichende Abstandsvergrößerung ist nicht möglich.

Als weitere Schutzmaßnahme kommt die Härtung des verwendeten Geräts in Frage. Gegen NEMP gehärtetes Gerät ist allerdings nur im militärischen Produktbereich verfügbar. Ziviles Geräte, insbesondere aktuelle Computer-, Netzwerk- und Bustechnik, besitzt keinen EMP-Schutz. Übliche Blitzschutzsysteme sind zum EMP-Schutz nicht ausreichend.

Sicherheit kann durch elektromagnetische Schirmung geschaffen werden, wobei das Gesamtsystem betrachtet werden muss. Die Schirmung einzelner Komponenten ist nicht ausreichend. Innerhalb eines geschirmten Raumes treten keine Feldstärken mehr auf, die gefährlich werden könnten. Somit können herkömmliche Systeme ohne Zusatzaufwand installiert, betrieben und modifiziert werden.

Maßnahmen

Die wichtigste Sofortmaßnahme für die Verantwortlichen ist eine Beschäftigung mit dem Thema – das Ignorieren einer potenziellen Gefahr kann zu einem unsanften Erwachen führen. Bei einer Analyse der Bedrohungsszenarien, der Verwundbarkeit, den möglicherweise auftretenden Schäden und deren wirtschaftlichen Auswirkungen sollte man sich von Fachleuten beraten lassen. Gleiches gilt für die Planung möglicher Schutzmaßnahmen. Eine Risikobewertung und die Abwägung von Sicherheitsaufwand zu Schadenshöhe müssen erfolgen. Bei einer Entscheidung für präventive Maßnahmen sollte unbedingt auf das Know-how von Fachfirmen zurückgegriffen werden. Gleiches gilt im Anschluss für den Test umgesetzter Maßnahmen. ■

Weiterführende Infos auf www.Sul24.net

more @ click SIK08452