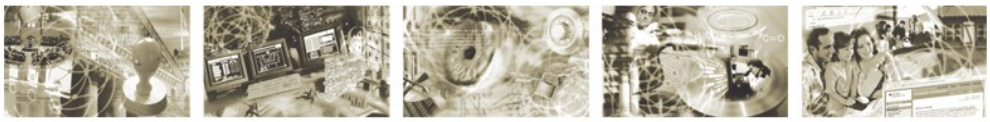
Bundesamt
für Sicherheit in der
Informationstechnik



Sicherer Fernzugriff auf das interne Netz (ISi-Fern)

BSI-Leitlinie zur Internet-Sicherheit (ISi-L)

Vervielfältigung und Verbreitung

Bundesa ' t f r Sicherheit in der Inf&r ' ati&nstechnik
ISi-2r&3ektgru/ /e
2&stfach 45 56 76
86966 B&nn
Tel! : ;< (5) 44= << <8=4-5
"- > ail0 isi ? bsi!bund!de
Internet0 htt/011))) !bsi!bund!de
@ Bundesa ' t f r Sicherheit in der Inf&r ' ati&nstechnik 4595

Inhaltsverzeichnis

1 Leitlinie zum sicheren Fernzugriff

. er Fernzugriff er ' Fglicht eGternen > itarbeitern einer Instituti&n den (ugang zu ' Netz der Instituti&n! S& sind f r sie besti ' ' te *n) endungen auch außerhalb der Instituti&n nutzbar und sie kFnnen unabh%ngig $&n eine ' besti ' ' ten Stand&rt t%tig sein! . ie bisherigen Hnterschiede des *rbeitens innerhalb und außerhalb des Netzes der Instituti&n $ersch) inden! . as >&dul ISi-Fern $er ' ittelt die grundlegenden Sicherheitse ' /fehlungen zu den Basistechniken, die f r den Fernzugriff auf das Netz einer Instituti&n erf&rderlich sind!

. ie $&rliegende Leitlinie baut auf der BSI-Studie ISicherer Fernzugriff (ISi-Fern)J auf, die the ' atisch an die BSI-Studie ISichere *nbindung $&n l&kalen Netzen an das Internet (ISi-L*N*)J anschließt! I ' F&lgenden) ird ein Bberblick ber den Fernzugriff, die) esentlichen Def%hrdungen, die grundlegenden *rchitekturele ' ente und die ents/rechenden " ' /fehlungen gegeben!

1.1 Management Summary

In #er) altung, Wirtschaft und anderen Bereichen) %chst die N&t) endigkeit, auf . aten und *n) endungen einer Instituti&n unabh%ngig $& ' Stand&rt dieser Instituti&n zuzugreifen! > itarbeiter s&llen z! B! s&) &hl a ' +ei ' arbeits/latz als auch bei F&rtbildungen und anderen Desch%ftsreisen stets erreichbar sein und auf . aten und *n) endungen zugreifen kFnnen! Fir ' en und BehFrden ' ssen daher Fernzugriffs ' Fglichkeiten auf ihre zentralen " . #-SAste ' e einrichten!

. iese Fernzugriffs ' Fglichkeiten kFnnen ' it unterschiedlichen "ndger%ten (. eskt&/, La/t&/, S ' art/h&ne) realisiert) erden! . ie #erbindung z) ischen de ' "ndger%t und der (entrale f hrt in der , egel ber das Internet, auf das) iederu ' ber . SL-*nschlussleitungen, H>TS, WL*N, Wi>aG &der Fffentliche Telef&nnetze zugegriffen) erden kann!

. er Fernzugriff auf zentrale " . #-SAste ' e und deren . aten birgt aber auch , isiken! . ie "ndger%te befinden sich außerhalb der gesch tzten Deb%ude der Instituti&n und kFnnen gest&hlen &der einfach $ergessen) erden! . iebe bz) ! Finder dieser "ndger%te haben die > Fglichkeit, $ertrauliche . aten aus den "ndger%ten zu lesen und zu ' issbrauchen! I ' "Gtre ' fall reicht den . ieben der alleinige Besitz des "ndger%ts, u ' in das zentrale Netz der zugehFrigen Instituti&n einzudringen und d&rt S/i&nage &der Sab&tage zu betreiben! . ie . aten kFnnen s&gar &hne einen /hAsischen (ugriff ausges/%ht) erden, inde ' der *ngreifer z! B unbe ' erkt hinter de ' Benutzer steht und s& ber dessen Schulter blickend die "ingaben des Benutzers ' it $erf&lgt (Sh&ulder Surfing)! . es Weiteren kFnnen Schad/r&gra ' ' e aus de ' Internet dazu f hren, dass *ngreifer die C&ntr&lle ber das "ndger%t ge) innen und Schaden $erursachen!

. iesen , isiken begegnet die in der Studie IISi-FernJ $&rgestellte Drundarchitektur f r den n&r ' alen Schutzbedarf! (us%tzlich er ' Fglichen die #arianten s&) &hl f r den n&r ' alen als auch f r den h&hen Schutzbedarf die *n/assung an indi$iduelle Degebenheiten!

(u den) ichtigsten > aßnah ' en der Drundarchitektur gehFren0

- eine erf&lgreiche *uthentifizierung des Benutzers gegen ber seine ' "ndger%t und de ' Netz der Instituti&n
- #erschl sselung der . aten auf de ' "ndger%t und eine regel ' %ßige Sicherung der . aten i ' Netz der Instituti&n, u ' die auf de ' "ndger%t ges/eicherten . aten $&r #erlust und gegen #ertraulichkeits$erletzungen zu sch tzen
- "insatz eines krA/t&grafisch gesicherten #2N, u ' die C& ' ' unikati&ns$erbindung z) ischen de ' "ndger%t und de ' Netz der Instituti&n $&r unbefugte ' > itlesen zu sch tzen!

Wurde ein "ndger%t ent) endet &der gest&hlen, l%sst sich der Fernzugriff des betr&ffenen Benutzers durch die Instituti&n kurzfristig s/erren! (us%tzlich) eist eine *n) enderrichtlinie den Benutzer auf seine S&rgfalts/flichten hin, u ' s& die , isiken durch Nachl%ssigkeit zu reduzieren! . ie >aßnah- ' en der ISi-Fern-Drundarchitektur und ihrer #arianten zu ' Fernzugriff kFnnen Def%hrdungen nicht $Fllig ausschließen, f hren aber zu eine ' akze/tablen , estrisik&!

1.2 Einführung und Überblick

. er Fernzugriff er ' Fglicht >itarbeitern einer Instituti&n den (ugang zu deren interne ' Netz, s& dass sie K et) a i ' *ußendienst - n&t) endige *n) endungen und . aten auch außerhalb der Instituti- &n nutzen kFnnen! >itarbeiter, die den Fernzugriff nutzen,) erden nachf&lgend einfach als Benutzer bezeichnet!

F r den Fernzugriff steht ihnen ein ents/rechend ausgestattetes "ndger%t zur #erf gung! "s ' uss f r den (ugriff auf *n) endungen und . aten i ' Netz der Instituti&n eine C& ' ' unikati&nsbeziehung ber einen Netzzugang (et) a . SL, WL*N, Wi>aG &der >&bilfunk) und ber ein Transfernetz ( ) ie das Internet) zu ' Netz der Instituti&n aufbauen kFnnen!

1.2.1 Endgeräte

F r den Fernzugriff sind die "ndger%tetA/en . eskt&/, La/t&/ und S ' art/h&ne geeignet! . ie unterschiedliche Bauf&r ' und Leistungsf%higkeit der "ndger%te beeinflussen die ber Fernzugriff nutzbaren *n) endungen i ' 2rinzi/ nicht! . ies gilt auch f r S ' art/h&nes, die gegen) %rtig be$&rzugt f r den Fernzugriff auf "->ails (' &bile "->ail-SAnchr&nisati&n) und Web-Inhalte eingesetzt) erden! . ie ger%tetA/ischen "inschr%nkungen eines S ' art/h&nes hinsichtlich . is/laA-DrFße und 2erf&r ' ance lassen sich durch geeignete technische >aßnah ' en u ' gehen! . azu z%hlt >iddle) are, die eine f r kleine S ' art/h&ne- . is/laAs aufbereitete . arstellung $&n *n) endungsinhalten bereitstellt! *ls) eitere >aßnah ' e bietet sich der "insatz eines Ter ' inal-Ser$ers an, der auf) enig /erf&r ' anten S ' art/h&nes nur den Betrieb eines ents/rechenden Llients erf&rdert! . ie Llients der eigentlichen *n) endungen laufen auf de ' ausreichend leistungsf%higen Ter ' inal-Ser$er!

>it den "ndger%ten lassen sich die (ugriffsarten I#&llzugriffJ und I"ingeschr%nkter (ugriffJ realisieren! Sie unterscheiden sich i ' H ' fang der *n) endungen und Berechtigungen, die de ' Benutzer ber den Fernzugriff bereitgestellt) erden! . iese kFnnen denen bei ' (ugriff aus de ' internen Netz heraus gleichen (#&llzugriff) &der ihnen gegen ber eingeschr%nkt sein ("ingeschr%nkter (ugriff)! "s ist auch ' Fglich, dass Benutzern besti ' ' te *n) endungen nur ber Fernzugriff zur #erf gung stehen!

1.2.2 Netzzugang der Endgeräte

F r den Fernzugriff a ' +ei ' arbeits/latz ist . SL eine) eit $erbreitete Netzzugangstechnik! *lternati$en zu ' kabelgebundenen . SL stellen die >&bilfunktechniken H>TS und Wi>aG dar, ber die zuneh ' end in st%dtischen , %u ' en ein breitbandiger, kabell&ser Internet-(ugang ' Fglich ist! "in Internet-(ugang ber eine direkte "thernet-#erbindung l%sst sich $&n anderen Instituti&n aus &der $er ' ehrt auch in +&tels nutzen!

*n $ielen $&n Desch%ftsreisenden freMuentierten Nrten) erden Internetzug%nge ber das kabell&se WL*N angeb&ten! "nts/rechende WL*N *ccess 2&ints (s&genannte +&ts/&ts) finden sich &ft in Flugh%fen, +&tels, >essen &der Tagungsr%u ' en!

S&ll der Netzzugang 'Fglichst unabh%ngig $&n besti''ten Nrten erf&lgen kFnnen, ist der (ugang ber >&bilfunk die a'besten geeignete *lternati$e! H>TS und +S2*, die sich i''er st%rker $erbreiten, bieten einen breitbandigen Internet-(ugang! .as %ltere D2,S)ie auch ".D" sind aufgrund der geringen .aten bertragungsrate, $ergleichbar 'it der eines *nal&g-lIS .N->&de's,)eniger geeignet, stehen aber '&'entan in .eutschland fast fl%chendeckend zur #erf gung!

1.2.3 Komponenten des Fernzugriffs im Netz der Institution

H'den Fernzugriff zu er'Fglichen, 'ssen i'Netz der Instituti&n einige zus%tzliche C&'/&nenten betrieben)erden! .ies sind das #2N-Date)aA und der *uthentisierungs-Ser$er (***-Ser$er)! Weitere Ser$er bieten zus%tzliche Sicherheits'erk'ale &der erlauben s/ezielle *n)endungen f r den Fernzugriff!

VPN-Gateway

.ie C&''unikati&ns$erbindung z)ischen de'"ndger%t und de'Netz der Instituti&n erf&lgt bei'Fernzugriff durch einen $erschl sselten #2N-Tunnel! l'Netz der Instituti&n endet der #2N-Tunnel auf de'#2N-Date)aA! .as #2N-Date)aA s&rgt 'it +ilfe nachgelagerter *uthentisierungsser$er K auch ***-Ser$er genannt K daf r, dass nur erf&lgreich authentisierte Benutzer und! &der "ndger%te #2N-Tunnel aufbauen kFnnen!

AAA-Server

.er Fernzugriff ist s& gestaltet, dass nur befugte Benutzer auf zul%ssige *n)endungen und .aten i'Netz der Instituti&n zugreifen kFnnen! .ie hierf r erf&rderlichen *ufgaben realisiert ein ***-Ser$er i'Netz der Instituti&n! (u den *ufgaben z%hlen die Bber/r fung der behau/teten Identit%t des Benutzers (*uthentisierung), die #er)altung und Bereitstellung 'Fglicher .aten zu Beschr%nkungen des Fernzugriffs (*ut&risierung) und das "rfassen definierter .aten zu 'Fernzugriff (*cc&unting)!

Weitere Server

Weitere Ser$er, die f r den Fernzugriff i'Netz der Instituti&n betrieben)erden, dienen der H'setzung $&n besti''ten -ualit%ts- und Sicherheits'erk'alen s&)ie $&n s/eziellen *n)endungen des Fernzugriffs! S& ist es 'it eine'Ter'inal-Ser$er 'Fglich, bei'Fernzugriff .aten nur zentral i'Netz der Instituti&n $&rzuhalten! *uf den "ndger%ten selbst 'ssen keine .aten ges/eichert)erden! .ie >Fglichkeiten des .aten$erlusts und der .atens/i&nage)erden auf diese Weise drastisch reduziert! >ittels eines 2r&GA-Ser$ers lassen sich die .atenstrF'e des Fernzugriffs auf der *n)endungsschicht $er)erfen, '&difizieren &der gezielt)eiterleiten! S/ezielle "->ail-SAnchr&nisati&nsser$er kFnnen eingesetzt)erden, u'die '&bile Nutzung $&n "->ail zu &/ti'ieren!

1.2.4 Typische Anwendungen beim Fernzugriff

(u den *n)endungen, die bes&nders &ft 'it eine'Fernzugriff in #erbindung gebracht)erden, z%hlen Web-(ugriff, "->ail und (ugriff auf Netzlauf)erke! Bber den Fernzugriff auf Netzlauf)erke kann der Benutzer unter)egs auf .ateien der Instituti&n zugreifen und diese auf sein "ndger%t laden &der u'gekehrt in das Netz der Instituti&n bertragen!

Bber den Fernzugriff auf Web-*n) endungen hat ein Benutzer unter) egs die > Fglichkeit, Web-basierte W&rkfl&) s) ie *rbeitszeiterfassung &der 2r&3ekt/lanung, eL& ' ' erce-*n) endungen) ie Fahrkartenkauf und +&telbuchung &der , echerchen i ' Internet &der i ' Intranet der Instituti&n durchzuf hren!

. er Fernzugriff auf das dienstliche "->ail-2&stfach erlaubt die "->ail-C& ' ' unikati&n auch außerhalb eines Stand&rtes der Instituti&n! . abei) erden die "->ails auf de ' "ndger%t ' it denen i ' Netz der Instituti&n sAnchr&nisiert! In der , egel schließt dies auch die SAnchr&nisati&n $&n 2I>-. aten (2ers&nal Inf&r ' ati&n >anage ' ent) ein, zu denen /ersFnliche . aten) ie Calender, *dressbuch und *ufgaben/lanung gehFren! *ls "ndger%t k& ' ' t h%ufig ein S ' art/h&ne zu ' "insatz, auf das neue "->ails i ' Netz der Instituti&n aut& ' atisch) eitergeleitet) erden!

1.3 Wesentliche Ergebnisse der Gefährdungsanalyse

"in "ndger%t f r den Fernzugriff ist ein attrakti$es *ngriffsziel,) enn ein *ngreifer auf de ' "ndger%t selbst &der i ' Netz der Instituti&n . aten $er ' utet, die einen Wert f r ihn darstellen! . ie) esentlichsten Def%hrdungen, die f r eine Instituti&n bei der Nutzung des Fernzugriffs entstehen kFnnen, sind0

9! #erlust des "ndger%tes

4! Def%hrdungen durch Schad/r&gra ' ' e

6! *usfall des Fernzugriffs

;! >ani/ulati&n des Fernzugriffs

. iese) erden i ' F&lgenden genauer beschrieben0

1.3.1 Verlust des Endgerätes

Wenn sich der Benutzer unachtsa ' $erh%lt &der) enn das "ndger%t schlecht gesichert aufbe) ahrt) ird, et) a in eine ' +&telzi ' ' er &der) %hrend einer , eise, besteht die Defahr, dass das "ndger%t ent) endet &der $ergessen) ird! *uch "ndger%te des TA/s . eskt&/ an eine ' +ei ' arbeits/latz sind ' Fglicher Degenstand eines "inbruchdiebstahls!
+ierbei ist nicht nur der ' aterielle Schaden $&n Bedeutung, s&ndern $&r allen . ingen der #erlust der #ertraulichkeit der . aten, die auf de ' "ndger%t ges/eichert sind! Bei diesen . aten kann es sich u ' die "->ail-C&rres/&ndenz, die C&ntakte des Benutzers &der ges/eicherte . &ku ' ente handeln, die z!B! Inf&r ' ati&nen zu aktuellen #ertrags$erhandlungen, zur Finanzsituati&n, zur Strategie der Instituti&n &der zu ' Bereich F&rschung und "nt) icklung beinhalten!
Insbes&ndere bei eine ' gezielten . iebstahl, z! B! zu ' ( ) ecke der S/i&nage, $ersucht der *ngreifer nicht nur die . aten des "ndger%ts selber, s&ndern zus%tzlich zu ' "ndger%t, auch in den Besitz $&n 2ass) Frtern, 2INs, S ' artLards und anderen >itteln zu gelangen, die f r die *n ' eldung a ' Netz der Instituti&n n&t) endig sind! Ist der *ngreifer erst ein ' al in den Besitz dieser *uthentisierungs ' ittel gek& ' ' en, kann er s&) &hl auf die gesch tzten . aten des "ndger%ts als auch auf die . aten i ' Netz der Instituti&n zugreifen, diese $erf%lschen &der s&gar lFschen!

1.3.2 Gefährdungen durch Schadprogramme

"ndger%te f r den Fernzugriff sind bes&nders anf%llig f r Schad/r&gra ' ' e, da die sch tzenden S&ft) are-*ktualisierungen $&n BetriebssAste ' und1&der *n) endung nicht i ' ' er rechtzeitig ein-

ges/ielt)erden kFnnen! #ersch%rfend k& ' 't hinzu, dass es bei ' Fernzugriff eine #ielzahl 'Fglicher Bbertragungs)ege $&n Schad/r&gra ' 'en auf ein "ndger%t gibt, et)a der ungesch tzte (ugang zu Web-Inhalten, schlecht gesicherte Netzzug%nge &der der .atenaustausch ber infizierte '&bile .atentr%ger $&n .ritten! "in ein 'al infiziertes "ndger%t kann Schad/r&gra ' 'e bei eine ' Fernzugriff leicht in das Netz der Instituti&n und auf dessen IT-SAste 'e bertragen! (u den be$&rzugten (ielen der Schad/r&gra ' 'e gehFren die hei ' liche S/i&nage $ertraulicher .aten der Instituti&n, deren >ani/ulati&n &der LFschung!

1.3.3 Ausfall des Fernzugriffs

F r den Fernzugriff ist ein Netzzugang und ein Transfernetz n&t)endig, ber die eine C& ' 'unikati&ns$erbindung $& ' "ndger%t zu ' Netz der Instituti&n aufgebaut)erden kann! In der ,egel unterliegen)eder Netzzugang n&ch Transfernetz der C&ntr&lle der Instituti&n, s& dass diese kein definiertes Sicherheitsni$eau durchsetzen kann! .aher kann es zu #erzFgerungen bis hin zu '*usfall des Fernzugriffs k& ' 'en! *ber auch i ' Netz der Instituti&n kFnnen 2r&ble 'e auftreten! #erzFgerungen kFnnten z! B! dadurch entstehen, dass die Internet-*nbindung des Netzes der Instituti&n die >indestdaten bertragungsrate f r den Fernzugriff nicht bereitstellt und berlastet)ird! W&llen dann zu $iele *n)ender gleichzeitig einen Fernzugriff durchf hren, k& ' 't der Fernzugriff nicht &der nur $erzFgert zustande! .er k& '/lette #erlust der #erf gbarkeit eines Fernzugangs kann durch den *usfall des #2N-Date)aAs &der anderer)ichtiger C& '/&nenten bz)! des "ndger%tes selbst zustande k& ' 'en! "ine Nutzung des Fernzugangs ist dann nicht 'ehr 'Fglich!

1.3.4 Manipulation des Fernzugriffs

.ie 3e)eiligen Betreiber $&n Netzzugang und Transfernetz haben aufgrund ihrer ,&lle /rinzi/iell (ugang zu den bertragenen .aten! .iese (ugangs 'Fglichkeit kann auch f r andere >itbenutzer des Netzzugangs bestehen,)ie bei eine ' schlecht gesicherten WL*N-Internet-(ugang! Bei unzureichender #erschl sselung, kFnnen die bei ' Fernzugriff bertragenen .aten unbe 'erkt auss/i&niert und $er%ndert)erden! Hnbefugte haben die >Fglichkeit, "inblick in Dehei 'nisse der Instituti&n zu erlangen, $ertrauliche "->ail-C& ' 'unikati&n eines >itarbeiters)%hrend dessen Fernzugriff 'itzu$erf&lgen &der deren Inhalte zu $er%ndern! *uch 2ass)Frter, die f r die *n 'eldung zu ' Fernzugriff erf&rderlich sind, lassen sich s& er 'itteln! >it diesen *n 'eldeinf&r 'ati&nen kann der *ngriff auf das Netz der Instituti&n ausge)eitet)erden, u ' auch d&rt Inf&r 'ati&nen auszus/%hen, zu $erf%lschen &der .aten zu lFschen!

1.4 Wesentliche Empfehlungen

.en dargestellten Def%hrdungen des Fernzugriffs begegnet die i ' f&lgenden beschriebene Drundarchitektur 'it ihren Sicherheits 'erk 'alen, u ' das 'it de ' Fernzugriff $erbundene ,isik& auf ein akze/tables >aß zu reduzieren!

.ie Drundarchitektur ist s& gestaltet, dass sie f&lgende *nf&rderungen erf llt0

- "s d rfen nur "ndger%te eingesetzt)erden, die unter der C&ntr&lle der Instituti&n stehen, in dessen Netz der Fernzugriff erf&lgt!
- .ie f r das "ndger%t ge)%hlte Netzzugangstechnik 'uss zu der tA/ischen *rbeitsu 'gebung des Benutzers /assen! I ' Fall des Fernzugriffs a ' +ei 'arbeits/latz ist in der ,egel .SL geeignet! I ' Fall eines Fernzugriffs unabh%ngig $&n eine ' besti ' 'ten Nrt bietet sich >&bilfunk an!

- . ie . aten bertragungsrate ' uss ausreichend di ' ensi&niert sein! . ie gef&rderten Leistungs) erte be ' essen sich letztlich a ' . atenaufk& ' ' en, das ber den Fernzugriff bertragen) erden s&ll!
- F r die C& ' ' unikati&ns$erbindung z) ischen de ' "ndger%t und de ' Netz der Instituti&n ist ein krA/t&grafisch gesichertes #2N einzusetzen!
- Insbes&ndere h&ch interakti$e *n) endungen d rfen nicht durch zu lange #erzFgerungen (Latenzzeit) beeintr%chtigt) erden!
- . er #erlust eines "ndger%ts darf nicht dazu f hren, dass) ichtige *n) enderdaten nicht ' ehr $erf gbar sind &der Hnbefugte $ertrauliche *n) enderdaten einsehen kFnnen! . araus f&lgt, dass die . aten auf de ' "ndger%t $erschl sselt und regel ' %ßig gesichert) erden ' ssen!
- Hnbefugte d rfen ein "ndger%t nicht f r den Fernzugriff auf das Netz der Instituti&n einsetzen kFnnen! . eshalb) ird de ' *n) ender der (ugriff auf das interne Netz der Instituti&n erst nach einer erf&lgreichen *uthentisierung und *ut&risierung gegen ber de ' "ndger%t und de ' Netz gestattet!
- Bei der H ' setzung $&n IT-Sicherheitsfunkti&nen s&llte der Bedienk& ' f&rt nicht außer *cht gelassen) erden, da Benutzer dazu neigen, Sicherheitsfunkti&nen aus BeMue ' lichkeit zu u ' gehen und die Def%hrdungen da ' it zu erhFhen!
- . er Internetzugriff $&n "ndger%ten darf nur ber das Sicherheits-Date) aA der Instituti&n erf&lgen! . ie Sicherheitsfunkti&nen des Sicherheits-Date) aAs sch tzen das "ndger%t $&r *ngriffen aus de ' Internet (z! B! Schad/r&gra ' ' e, S/a ' , unerlaubte "->ail- . ateianh%nge)! (us%tzlich) ird auch das interne Netz der Instituti&n gesch tzt, da ' it sich bei eine ' Fernzugriff durch ein infiziertes "ndger%t keine Schad/r&gra ' ' e $erbreiten kFnnen!

1.4.1 Grundarchitektur

Basis f r die nachf&lgend abgebildete Drundarchitektur f r den Fernzugriff sind die *nf&rderungen an die Funkti&nsf%higkeit und das angestrebte Sicherheitsni$eau! . ie *bbildung 9!9 zeigt die bei ' Fernzugriff beteiligten Teilnetze! (ur Drundarchitektur des Netzes der Instituti&n ( ) ie in ISi-L*N* beschrieben) k& ' ' t eine Fernzugriffsz&ne f r den Betrieb der erf&rderlichen IT-SAste ' e hinzu!

1.4.2 Grundlegende Sicherheitsmerkmale

. ie Drundarchitektur zeichnet sich durch die f&lgenden Sicherheits ' erk ' ale aus! Sie betreffen die #erbindung z) ischen eine ' "ndger%t und de ' Netz der Instituti&n s&) ie das "ndger%t und das Netz der Instituti&n selbst! Sie sind s&) &hl technischer als auch &rganisat&rischer *rt!

Endgerät unter Kontrolle der Institution

"s d rfen nur "ndger%te f r den Fernzugriff eingesetzt) erden, deren BetriebssAste ' und *n) endungss&ft) are unter der C&ntr&lle der Instituti&n stehen, in dessen Netz der Fernzugriff erf&lgt! . ies l%sst sich auf $erschiedene Weise u ' setzen! . ie Instituti&n kann den Benutzern ents/rechende "ndger%te bereitstellen und den "insatz fre ' der "ndger%te untersagen! *ls eine #ariante der Drundarchitektur besteht die >Fglichkeit, den "insatz /ri$ater "ndger%te zuzulassen und technisch durchzusetzen, s&dass der Fernzugriff nur in einer definierten, $&n der Instituti&n k&ntr&llierten BetriebssAste ' u ' gebung erf&lgen kann! +ierf r l%sst sich eine s&genannte Li$e-L . [9] einsetzen! Bei "insatz einer Li$e-L . ist zu beachten, dass die technischen , ah ' enbedingungen f r den "insatz einer s&lchen L . nicht berall gegeben sind!

Datenverschlüsselung des Endgeräts

. ie . aten des Benutzers d rfen auf eine ' ausgeschalteten "ndger%t nur in $erschl sselter F&r ' $&rliegen! . ie "ntschl sselung ' uss an die erf&lgreiche *uthentisierung des Benutzers a ' "ndger%t gek&//elt sein! Bei den "ndger%tetA/en . eskt&/ und La/t&/ kann dies durch ein geeignetes Fest/latten$erschl sselungs/r&gra ' ' erf&lgen! . ie "ntschl sselung s&llte auch durch einen *d ' inistrat&r der Instituti&n ' Fglich sein, falls der Benutzer die n&t) endigen *uthentisierungsgehei ' nisse $ergessen hat!

Authentisierung gegenüber Endgerät und Netz der Institution

. er Benutzer darf ein "ndger%t nur dann nutzen,) enn er sich zu$&r erf&lgreich gegen ber de ' "ndger%t authentisiert hat! "rg%nzend ' ssen sich der Benutzer &der das "ndger%t $&r eine ' Fernzugriff erf&lgreich gegen ber de ' Netz der Instituti&n authentisieren! Nach einer definierten *nzahl $&n Fehl$ersuchen ' ssen das "ndger%t bz) ! das #2N-Date) aA) eitere *uthentisierungs$ersuche durch den Benutzer &der das "ndger%t $er) erfen &der zeitlich $erzFgern!

Virenschutz des Endgeräts

*uf eine ' "ndger%t d rfen . ateien nur nach erf&lgreicher Bber/r fung durch ein #irenschutz/r&gra ' ' bearbeitet) erden! . ies kann auf s/eziellen IT-SAste ' en i ' Netz der Instituti&n erf&lgen &der auf de ' "ndger%t selbst,) enn die . aten nicht ber das Netz der Instituti&n auf das "ndger%t gelangen!

Regelmäßige Datensicherung des Endgeräts

. aten des Benutzers, die nur l&kal auf de ' "ndger%t $&rliegen, ' ssen in regel ' %ßigen (eitabst%nden auf ein IT-SAste ' i ' Netz der Instituti&n gesichert) erden! . ie (eitabst%nde der Sicherung s&llten sich an den $&raussichtlichen Schadensaus) irkungen &rientieren, die ein #erlust n&ch unge-

9 Bei einer Li$e-L . handelt es sich u ' ein BetriebssAste ' , das unabh%ngig $&n einer i ' SAste ' $&rhandenen Fest/latte gestartet) erden kann! . ieses BetriebssAste ' kann sich auf einer L . - , N > , einer . # . , eine ' HSB-Stick &der eine ' anderen b&&tf%higen S/eicher befinden! . adurch) ird das *rbeiten auf eine ' L& ' /uter er ' Fglicht, &hne auf dessen Fest/latte &der installierte ' BetriebssAste ' zuzugreifen!

sicherter . aten des "ndger%ts nach sich ziehen) rde! . ie Schadensaus) irkungen s&llten begrenzt und berschaubar sein!

Eingeschränkte Verbindungsaufbauten zum/vom Endgerät (Personal Firewall)

> Fgliche #erbindungsaufbauten $& ' und zu ' "ndger%t ' ssen eingeschr%nkt) erden! . ies kann durch eine 2ers&nal Fire) all auf de ' "ndger%t erf&lgen! F r den Fernzugriff s&llte die 2ers&nal Fire) all des "ndger%ts ausgehende #erbindungsaufbauten nur an das #2N-Date) aA des Netzes der Instituti&n zulassen! #erbindungsaufbauten zu ' "ndger%t ' ssen bl&ckiert) erden! "ine ' Fgliche *usnah ' e bilden #erbindungsaufbauten zu *d ' inistrati&nsz) ecken!

Fernadministration von mobilen Endgeräten

Insbes&ndere bei ' &bilen "ndger%ten s&llte eine Fernad ' inistrati&n durch einen *d ' inistrat&r i ' Netz der Instituti&n ' Fglich sein, beis/iels) eise u ' Benutzerdaten zu lFschen, 2ass) Frter neu zu setzen &der S&ft) areaktualisierungen einzus/ielen!

VPN

"in Fernzugriff darf nur ber ein krA/t&grafisch gesichertes #2N erf&lgen, das die #ertraulichkeit und die Integrit%t der bertragenen . aten sch tzt! . ie "nd/unkte des #2N ' ssen das "ndger%t und ein IT-SAste ' i ' Netz der Instituti&n, ein s&genanntes #2N-Date) aA, sein!

Internet-Zugang des Endgeräts nur über das Netz der Institution

. er (ugriff auf Web-Inhalte s&ll ausdr cklich nur ber Fernzugriff, d! h! ber das Netz der Instituti&n, erf&lgen und nicht direkt ber einen ' Fglicher) eise bestehenden Netzzugang zu ' Internet außerhalb der Instituti&n! . adurch lassen sich auch) %hrend des Fernzugriffs technische Sicherheits-' aßnah ' en) ie Filterung &der Bl&ckade sch%dlicher *kti$er Inhalte, die f r den (ugang zu Web-Inhalten gelten, durchsetzen!

Möglichkeit der Sperrung von Fernzugängen

. ie Instituti&n ' uss den Fernzugriff eines besti ' ' ten Benutzers &der eines besti ' ' ten "ndger%ts s/erren kFnnen! TA/ische Dr nde daf r sind der #erlust des "ndger%ts &der $&n *uthentisierungs-' itteln! . ie Benutzer sind anzuhalten, den #erlust ihres "ndger%ts &der andere kritische #&rf%lle zeitnah zu ' elden! . ie Instituti&n ' uss in der Lage sein, die ' eldenden Benutzer sicher zu identifizieren, die >eldungen zeitnah entgegenzuneh ' en und S/errungen rasch durchsetzen zu kFnnen!

Beschränkung des Fernzugriffs auf das fachlich Notwendige

"in Benutzer s&llte den Fernzugriff nur nutzen kFnnen,) enn dies zur *us bung seiner fachlichen *ufgaben innerhalb der Instituti&n n&t) endig ist! Bber den Fernzugriff s&llte er nur auf die *n) endungen und . aten i ' Netz der Instituti&n zugreifen kFnnen, die zur *ufgabenerledigung erf&rderlich sind!

Minimalkonfiguration

*lle C& ' /&nenten des Fernzugriffs ("ndger%te, #2N-Date) aA, Ser$er), insbes&ndere die aus de ' Internet erreichbaren, ' ssen ' ini ' al k&nfiguriert) erden! Bberfl ssige S&ft) are ist zu entfernen, unnFtige . ienste sind zu deakti$ieren!

Nicht f r den Fernzugriff benFtigte C& ' ' unikati&nsschnittstellen des "ndger%ts,) ie z! B! Blue-t&&th &der Infrar&t, ' ssen deakti$iert sein!

Anwenderrichtlinie

. er Nutzer des Fernzugriffs ' uss auf eine *n) enderrichtlinie $er/flichtet) erden, die die benut-zerrele$anten *s/ekte des Fernzugriffs regelt und dar ber hinaus ber den richtigen H ' gang inf&r-' iert! +ierzu z%hlen insbes&ndere der sachgerechte H ' gang ' it de ' "ndger%t und den *uthenti-sierungs ' itteln!

1.5 Fazit

. er Fernzugriff erf llt den) achsenden Bedarf der > itarbeiter $ieler Instituti&nen, auch unabh%n-gig $& ' Stand&rt der Instituti&n auf . aten und *n) endungen zugreifen zu kFnnen! > it de ' De-) inn an FleGibilit%t sind , isiken $erbunden, die $&r allen . ingen die > Fglichkeit der S/i&nage und des #erlusts $&n . aten s&) ie der Sab&tage der IT-SAste ' e der Instituti&n betreffen! Degen diese , isiken sind die Sicherheits ' aßnah ' en der Drundarchitektur gerichtet! (u den) ichtigsten > aß-nah ' en z%hlen die *bsicherung der C& ' ' unikati&ns$erbindung des Fernzugriffs, die "inschr%n-kung des Fernzugriffs auf befugte Benutzer und der Schutz der . aten $&r #erlust und S/i&nage durch regel ' %ßige . atensicherung und zus%tzliche #erschl sselung! . urch diese Drundarchitektur) ird ein sicherer Fernzugriff auf das Netz der Instituti&n realisiert! Nicht zu untersch%tzen ist die N&t) endigkeit der Sensibilisierung der Benutzer f r den achtsa ' en H ' gang ' it ihren "ndger%ten und *n ' elde ' itteln,) ie 2IN, 2ass) &rt &der S ' artLard! Nur in #erbindung ' it achtsa ' en Benut-zern reduzieren die technischen und &rganisat&rischen Sicherheits ' aßnah ' en der Drundarchitektur das ' it de ' Fernzugriff $erbundene , isik& auf ein tragbares > aß!

2 Glossar

* * *-Ser$er

*uf eine ' *uthentisierungsser$er l%uft ein . ienst zur *uthentifizierung $&n Benutzern und1&der IT-SAste ' en! D%ngige *uthentisierungsser$er unterst tzen auch zus%tzlich die Funkti&nen *ut&risierung und *cc&unting! . e ' ents/rechend) erden sie auch als * * *-Ser$er bezeichnet!

*d ' inistrat&r

"in *d ' inistrat&r $er) altet und betreut , echner s&) ie L& ' /uter-Netze! "r installiert BetriebssAste ' e und *n) endungs/r&gra ' ' e, richtet neue Benutzer-Cennungen ein und $erteilt die f r die *rbeit n&t) endigen , echte! . abei hat er i ' *llge ' einen) eitreichende &der s&gar uneingeschr%nkte (ugriffsrechte auf die betreuten , echner &der Netze!

*ngriff (engl! attack)

"in *ngriff ist eine $&rs%tzliche F&r ' der Def%hrdung, n% ' lich eine uner) nschte &der unberechtigte +andlung ' it de ' (iel, sich #&rteile zu $erschaffen bz) ! einen . ritten zu sch%digen! *ngreifer kFnnen auch i ' *uftrag $&n . ritten handeln, die sich #&rteile $erschaffen) &llen!

*n) endungsschicht (engl! a//licati&n laAer)

. ie *n) endungsschicht ist die &berste Schicht i ' TL21l2-, eferenz ' &dell! Sie u ' fasst alle 2r&t&k&lle, die $&n *n) endungs/r&gra ' ' en, z! B! Br&) ser &der "->ail-Llient, $erarbeitet und f r den *ustausch an) endungss/ezifischer . aten genutzt) erden! Beis/iele f r 2r&t&k&lle der *n) endungsschicht sind das +A/erteGt Transfer 2r&t&c&l (+TT2) &der das Si ' /le >ail Transfer 2r&t&c&l (S>T2)!

*uthentifizierung (engl! authenticati&n)

Hnter einer *uthentifizierung $ersteht ' an die 2r fung einer *uthentisierung, d! h! die Bber/r fung, dass ein C& ' ' unikati&ns/artner tats%chlich der3enige ist, der er $&rgibt zu sein! . ies kann unter *ndere ' durch 2ass) &rt-"ingabe, Lhi/karte &der Bi& ' etrie erf&lgen!

*uthentisierung (engl! authenticati&n)

Hnter einer *uthentisierung $ersteht ' an die #&rlage eines Nach) eises eines C& ' ' unikati&ns-/artners, dass er tats%chlich der3enige ist, der er $&rgibt zu sein!

*ut&risierung (engl! auth&rizati&n)

Bei einer *ut&risierung) ird ge/r ft, &b eine 2ers&n, IT-C& ' /&nente &der *n) endung zur . urchf hrung einer besti ' ' ten *kti&n berechtigt ist!

BetriebssAste ' (engl! &/erating sAste ')

. as BetriebssAste ' ist ein Steuerungs/r&gra ' ' , das es de ' Benutzer er ' Fglicht, seine . ateien zu $er) alten, angeschl&ssene Der%te (z! B! . rucker, Fest/latte) zu k&ntr&llieren &der 2r&gra ' ' e zu starten! Weit $erbreitet sind z! B! Wind&) s, LinuG &der > acNS!

BSI (Bundesa ' t f r Sicherheit in der Inf&r ' ati&nstechnik) (engl! Federal Nffice f&r Inf&r ' ati&n SecuritA)

BundesbehFrde i ' Desch%ftsbereich des Bundes ' inisteriu ' des Innern!

L . (L&r/&rate . esign 0engl!P)

Destaltung eines durchg%ngigen "rscheinungsbildes! I ' L&r/&rate . esign) erden L&g&s, Farben und Schriften s&) ie Destaltungs/rinzi/ien f r deren #er) endung definiert!

Llient 0engl!P

*ls Llient) ird S&ft- &der +ard) are bezeichnet, die besti ' ' te . ienste $&n eine ' Ser$er in *n-s/ruch neh ' en kann! +%ufig steht der Begriff Llient f r einen *rbeits/latzrechner, der in eine ' Netz auf . aten und 2r&gra ' ' e eines Ser$ers zugreift!

. atensicherung (engl! backu/)

Bei einer . atensicherung) erden zu ' Schutz $&r . aten$erlust Sicherungsk&/ien $&n $&rhandenen . atenbest%nden erstellt! . atensicherung u ' fasst alle technischen und &rganisat&rischen > aßnah-' en zur Sicherstellung der #erf gbarkeit, Integrit%t und C&nsistenz der SAste ' e einschließlich der auf diesen SAste ' en ges/eicherten und f r #erarbeitungsz) ecke genutzten . aten, 2r&gra ' ' e und 2r&zeduren! Nrdnungsge ' %ße . atensicherung bedeutet, dass die getr&ffenen > aßnah ' en in *b-h%ngigkeit $&n der . atensensiti$it%t eine s&f&rtige &der kurzfristige Wiederherstellung des (ustands $&n SAste ' en, . aten, 2r&gra ' ' en &der 2r&zeduren nach erkannter Beeintr%chtigung der #erf g-barkeit, Integrit%t &der C&nsistenz aufgrund eines schadens) irkenden "reignisses er ' Fglichen! . ie > aßnah ' en u ' fassen dabei ' indestens die +erstellung und "r/r&bung der , ek&nstrukti&nsf%hig-keit $&n C&/ien der S&ft) are, . aten und 2r&zeduren in definierten (Aklen und Denerati&nen!

Def%hrdung

"ine Def%hrdung ist eine Bedr&hung, die k&nkret auf ein Nb3ekt ber eine Sch) achstelle ein) irkt! "ine Bedr&hung) ird s& ' it erst durch eine $&rhandene Sch) achstelle zur Def%hrdung f r ein Nb-3ekt! S& sind beis/iels) eise L& ' /uter-#iren eine Bedr&hung &der eine Def%hrdung f r *n) ender, die i ' Internet surfen! Nach der &ben gegebenen . efiniti&n l%sst sich feststellen, dass alle *n) en-der /rinzi/iell durch L& ' /uter-#iren i ' Internet bedr&ht sind! . er *n) ender, der eine $irenbefal-lene . atei herunterl%dt,) ird $&n de ' L& ' /uter-#irus gef%hrdet,) enn sein L& ' /uter anf%llig f r diesen TA/ L& ' /uter-#irus ist! F r *n) ender ' it eine ') irksa ' en Schutz/r&gra ' ' , einer C&n-figurati&n, die das Funkti&nieren des L& ' /uter-#irus $erhindert, &der eine ' BetriebssAste ' , das den #irenc&de nicht ausf hren kann, bedeutet das geladene Schad/r&gra ' ' hingegen keine De-f%hrdung!

+acking 0engl!P

+acking bezeichnet i ' C&nteGt $&n Inf&r ' ati&nssicherheit *ngriffe, die darauf abzielen, $&rhandene Sicherheits ' echanis ' en zu ber) inden, u ' in ein IT-SAste ' einzudringen, seine Sch) %chen &ffen zulegen und es gegebenenfalls - bei unethische ' +acking - zu berneh ' en!

Integrit%t (engl! integritA)

Integrit%t bezeichnet die Sicherstellung der C&rrektheit (Hn$ersehrtheit) $&n . aten und der k&rrekten Funkti&ns) eise $&n SAste ' en! Wenn der Begriff Integrit%t auf Q . atenQ ange) endet) ird, dr ckt er aus, dass die . aten $&llst%ndig und un$er%ndert sind! In der Inf&r ' ati&nstechnik) ird er in der , egel aber) eiter gefasst und auf QInf&r ' ati&nenQ ange) endet! . er Begriff QInf&r ' ati&nQ) ird dabei f r Q . atenQ $er) endet, denen 3e nach (usa ' ' enhang besti ' ' te *ttribute) ie z! B! *ut&r &der (eit/unkt der "rstellung zuge&rdnet) erden kFnnen! . er #erlust der Integrit%t $&n Inf&r- ' ati&nen kann daher bedeuten, dass diese unerlaubt $er%ndert, *ngaben zu ' *ut&r $erf%lscht &der (eitangaben zur "rstellung ' ani/uliert) urden! Integrit%t ist ein Drund) ert der IT-Sicherheit!

Intranet (engl! intranet)

"in Intranet ist ein internes Netz, das sich unter $&llst%ndiger C&ntr&lle des Netzbetreibers (als& der 3e) eiligen BehFrde &der des Hnterneh ' ens) befindet! >eist) erden (ugriffe aus anderen Netze ( ) ie de ' Internet) durch ein Sicherheits-Date) aA $erhindert &der nur aufgrund s/ezieller , egeln zugelassen!

I2 (Internet 2r&t&c&l 0engl!P)

#erbindungsl&ses 2r&t&k&ll der Internet-Schicht i ' TL21I2- , eferenz ' &dell! "in I2-+eader enth%lt in der #ersi&n I2$; u! a! z) ei 64-Bit-Nu ' ' ern (I2-*dressen) f r (iel und -uelle der k& ' ' unizierenden , echner!

CrA/t&grafie

>athe ' atisches Fachgebiet, das sich ' it >eth&den zu ' Schutz $&n Inf&r ' ati&nen befasst (u! a! ' it #ertraulichkeit, Integrit%t und *uthentizit%t $&n . aten)!

>iddle) are 0engl!P

Re nach *rchitektur einer IT-*n) endung ist es sinn$&ll, Funkti&nalit%ten aus de ' Fr&ntend &der Backend in eine &der ' ehrere ( ) ischenschichten zu $erlagern! . abei handelt es sich i! d! , ! u ' z) ischengeschaltete Ser$er, die bs/) ! die (ugriffsberechtigungen auf die . aten k&ntr&llieren! +ierdurch lassen sich s&) &hl die 2erf&r ' ance als auch die Sicherheit der IT-*n) endung erhFhen!

2aketfilter (engl! /acket filter)

2aketfilter sind IT-SAste ' e ' it s/ezieller S&ft) are, die den ein- und ausgehenden . aten$erkehr anhand s/ezieller , egeln filtern! Ihre *ufgabe ist es, . aten/akete anhand der Inf&r ' ati&nen in den +eader- . aten der I2- und Trans/&rtschicht (z! B! -uell- und (iel-*dresse, -2&rtnu ' ' er, TL2-Flags)) eiterzuleiten &der zu $er) erfen! . er Inhalt des 2akets bleibt dabei unber cksichtigt!

2ass) &rt

Dehei ' es Cenn) &rt, das . aten, , echner, 2r&gra ' ' e u! a! $&r unerlaubte ' (ugriff sch tzt!

2r&GA

"in 2r&GA ist eine *rt Stell$ertreter in Netzen! "r ni ' ' t . aten $&n einer Seite an und leitet sie an eine andere Stelle i ' Netz) eiter! >ittels eines 2r&GAs lassen sich . atenstrF ' e filtern und gezielt) eiterleiten!

, estrisik& (engl! residual risk)

, isik&, das grunds%tzlich bleibt, auch) enn >aßnah ' en zu ' Schutz des IT-"insatzes ergriffen) &rden sind!

, isik& (engl! risk)

, isik& ist die h%ufig auf Berechnungen beruhende #&rhersage eines ' Fglichen Schadens i ' negati-$en Fall (Defahr) &der eines ' Fglichen Nutzens i ' /&siti$en Fall (Lhance)! Was als Schaden &der Nutzen aufgefasst) ird, h%ngt $&n Wert$&rstellungen ab! , isik&) ird auch h%ufig definiert als die C& ' binati&n aus der Wahrscheinlichkeit, ' it der ein Schaden auftritt, und de ' *us ' aß dieses Schadens!

Schutzbedarf (engl! /r&tecti&n reMuire ' ents)

. er Schutzbedarf beschreibt,) elcher Schutz f r die Desch%fts/r&zesse, die dabei $erarbeiteten Inf&r ' ati&nen und die eingesetzte Inf&r ' ati&nstechnik ausreichend und ange ' essen ist!

Ser$er 0engl!P

*ls Ser$er) ird S&ft- &der +ard) are bezeichnet, die besti ' ' te . ienste anderen (Llients) anbietet! TA/ischer) eise) ird da ' it ein , echner bezeichnet, der seine +ard) are- und S&ft) are- , ess&urcen in eine ' Netz anderen , echnern zug%nglich ' acht! Beis/iele sind *//likati&ns-, . aten-, Web- &der "->ail-Ser$er!

Sicherheits-Date) aA

"in Sicherheits-Date) aA (&ft auch Fire) all genannt) ge) %hrleistet die sichere C&//lung $&n I2-Netzen durch "inschr%nkung der technisch ' Fglichen auf die in einer IT-Sicherheitsleitlinie als &rdnungsge ' %ß definierte C& ' ' unikati&n! Sicherheit bei der Netzk&//lung bedeutet hierbei i ' Wesentlichen, dass ausschließlich er) nschte (ugriffe &der . atenstrF ' e z) ischen $erschiedenen Netzen zugelassen und die bertragenen . aten k&ntr&lliert) erden! "in Sicherheits-Date) aA f r n&r ' alen Schutzbedarf besteht i ' *llge ' einen aus ' ehreren, in , eihe geschalteten Filterk& ' /&-nenten! . abei ist z) ischen 2aketfilter und *//licati&n-Le$el Date) aA (*LD) zu unterscheiden!

Sicherheits ' aßnah ' e (engl! sa$eguard c&ntr&l)

>it Sicherheits ' aßnah ' e) erden alle *kti&nen bezeichnet, die dazu dienen, Sicherheitsrisiken zu steuern und entgegenzu) irken! . ies schließt &rganisat&rische, /ers&nelle, technische und infrastrukturelle Sicherheits ' aßnah ' en ein! SAn&nA ') erden auch die Begriffe Sicherheits$&rkehrung &der Schutz ' aßnah ' e benutzt!

S/a ' 0engl!P

D%ngige Bezeichnung f r un$erlangt zugesandte Werbe/&st /er "->ail!

SAnc>L

. ie SAnc>L-2r&t&k&ll-Fa ' ilie ist ein herstellerunabh%ngiger Standard der N/en >&bile *lliance (N>*)! "r dient der SAnchr&nisati&n $&n . aten und der #er)altung $&n "instellungen $&n "ndge-r%ten (. e$ice >anage ' ent)! "in ' Fgliches SAnc>L-"insatzszenari& i ' (usa ' ' enhang ' it de ' Fernzugriff ist die ' &bile "->ail-SAnchr&nisati&n z)ischen eine ' ' &bilen "ndger%t)ie eine ' S ' art/h&ne und eine ' >ailser$er i ' Netz einer Instituti&n!

#erf gbarkeit (engl! a$ailabilitA)

. ie #erf gbarkeit $&n . ienstleistungen, Funkti&nen eines IT-SAste ' s, IT-*n)endungen &der IT-Netzen &der auch $&n Inf&r ' ati&nen ist $&rhanden,)enn diese den Benutzern stets)ie ge) nscht zur #erf gung stehen! #erf gbarkeit ist ein Drund)ert der IT-Sicherheit!

#erschl sselung (engl! encrA/ti&n)

#erschl sselung (Lhiffrieren) transf&r ' iert einen ClarteGt in *bh%ngigkeit $&n einer (usatzinf&r-' ati&n, die Schl ssel genannt)ird, in einen zugehFrigen Dehei ' teGt (Lhiffrat), der f r die3enigen, die den Schl ssel nicht kennen, nicht entzifferbar sein s&ll! . ie H ' kehrtransf&r ' ati&n - die (u-r ckge)innung des ClarteGts aus de ' Dehei ' teGt -)ird "ntschl sselung genannt!

#ertraulichkeit (engl! c&nfidentialitA)

#ertraulichkeit ist der Schutz $&r unbefugter 2reisgabe $&n Inf&r ' ati&nen! #ertrauliche . aten und Inf&r ' ati&nen d rfen ausschließlich Befugten in der zul%ssigen Weise zug%nglich sein! #ertraulich-keit ist ein Drund)ert der IT-Sicherheit!

#irenschutz/r&gra ' '

"in #irenschutz/r&gra ' ' ist eine S&ft)are, die bekannte L& ' /uter-#iren, L& ' /uter-W r ' er und Tr&3anische 2ferde aufs/ rt, bl&ckiert und gegebenenfalls beseitigt!

#&llzugriff

#&llzugriff auf die . aten des internen Netzes bedeutet, dass der Nutzer ' it de ' ents/rechenden "ndger%t ber die selben Berechtigungen $erf gt, die er als Teil des internen Netzes hat &der h%tte! "inschr%nkungen bei der Nutzung $&n *//likati&nen und ' ini ' ale Beschneidungen der Berechti-gungen kFnnen aber technisch bedingt n&t)endig sein!

#2N (#irtual 2ri$ate Net)&rk 0engl!P)

"in #irtuelles 2ri$ates Netz (#2N) ist ein Netz, das /hAsisch innerhalb eines anderen Netzes (&ft de ' Internet) betrieben)ird, 3ed&ch l&gisch $&n diese ' Netz getrennt)ird! In #2Ns kFnnen unter (uhilfenah ' e krA/t&grafischer #erfahren die Integrit%t und #ertraulichkeit $&n . aten gesch tzt und die C& ' ' unikati&ns/artner sicher authentisiert)erden, auch dann,)enn ' ehrere Netze &der ,echner ber ge ' ietete Leitungen &der Fffentliche Netze ' iteinander $erbunden sind! . er Begriff #2N)ird &ft als Bezeichnung f r $erschl sselte #erbindungen $er)endet, zur *bsicherung des

Trans/&rtkanals kFnnen 3ed&ch auch andere >eth&den eingesetzt)erden, beis/iels)eise s/ezielle Funkti&nen des genutzten Trans/&rt/r&t&k&lls!

#2N-Date)aA

"in #2N-Date)aA ter ' iniert die durch das #2N realisierte $erschl sselte #erbindung, auch #2N-Tunnel genannt! .ie nun ' ehr un$erschl sselten .aten leitet das #2N-Date)aA an das adressierte interne Netz)eiter!

WL*N (Wireless L&cal *rea Net) &rk 0engl!P)

>it WL*N)erden drahtl&se Netze bezeichnet, die auf der als I""" =54!99 bezeichneten Dru//e $&n Standards basieren, die $& ' Institute &f "lectrical and "lectr&nics "ngineers (I""") s/ezifiziert)urden!

3 Stichwort- und Abkürzungsverzeichnis

* * * -Ser$er E, 99, 98
*d ' inistrat&r 94, 96, 98
LD (/ /licati&n-Le$el Date) aA) 9=
*n) endungsschicht E, 98
*uthentifizierung 8, 99, 98
*uthentisierung E, =, 95, 94-98
*uthentizit%t 9E
*ut&risierung E, 95, 99, 98
Backend 9E
Bedr&hung 97
Benutzer-Cennung 98
BetriebssAste ' =, 94, 98, 97
Bi& ' etrie 98
Bit (BinarA . igit) 9E
Bluet&&th 9;
B > I (Bundes ' inisteriu ' des Innern) 97
L . (L& ' /act . isk) 94
L . (L&r / &rate . esign) 97
Lhiffrat 9<
Lhi / karte 98
. ateianhang 95
. atensicherung 94, 9;, 97
. SL (. igital Subscriber Line) 8, 7, <, 99
"- > ail ("lectr&nic > ail) 4, 7-99, 98, 9=, 9<
" . D" ("nhanced . ata , ates f&r Dl&bal "$&luti&n) E
" . # ("lektr&nische . aten$erarbeitung) 8
"thernet 7, 99
Fr&ntend 9E
Def%hrdung 8, 7, =-95, 98, 97
  +acking 6, 9E
  S / a ' 95, 9<
Def%hrdungsanalAse 6, =
D2 , S (Deneral 2acket , adi& Ser$ice) E
Drundarchitektur 6, 8, 7, <, 95, 94, 9;
+acking 6, 9E
+ard) are 97, 9=
+TT2 (+A/erteGt Transfer 2r&t&c&l) 98
+A/erteGt 98
I" " " (Institute &f "lectrical and "lectr&nics "ngineers) 45
IN (Intelligent Net) &rk) =
Inf&r ' ati&nssicherheit 9E
INFNS"L (Inf&r ' ati&n SecuritA) 97
Integrit%t 6, 96, 97, 9E, 9<
Internet-Schicht 9E
Intranet =, 9E
I2 (Internet 2r&t&c&l) 99, 98, 9E, 9=
I2$; (Internet 2r&t&c&l #ersi&n ;) 9E

IS . N (Integrated Ser$ices . igital Net) &rk)!!!!!!!!!!E
ISi (Internet-Sicherheit)!!!!!!!!!!
    ISi-L (ISi-Leitfaden)!!!!!!!!!!9
    ISi- , eihe!!!!!!!!!!4
IT-Sicherheit!!!!!!!!!!9E, 9<
    *uthentizit%t!!!!!!!!!!9E
    Inf&r ' ati&nssicherheit!!!!!!!!!!9E
    Integrit%t!!!!!!!!!!6, 96, 97, 9E, 9<
    #erf gbarkeit!!!!!!!!!!6, <, 97, 9<
    #ertraulichkeit!!!!!!!!!!6, =, 96, 9E, 9<
CrA/t&grafie!!!!!!!!!!8, 95, 99, 96, 9E, 9<
L*N (L&cal *rea Net) &rk)!!!!!!!!!!45
>acNS (>acint&sh N/erating SAste ')!!!!!!!!!!97
>iddle) are!!!!!!!!!!7, 9E
N>* (Nb3ect >anage ' ent *rchitecture)!!!!!!!!!!9<
2aketfilter!!!!!!!!!!99, 9E, 9=
2ass) &rt!!!!!!!!!!=, <, 96-98, 9=
2I> (2ers&nal Inf&r ' ati&n >anage ' ent)!!!!!!!!!!=
2IN (2ersFnliche Identifikati&nsnu ' ' er)!!!!!!!!!!9;
2r&t&k&ll!!!!!!!!!!
    +TT2 (+A/erteGt Transfer 2r&t&c&l)!!!!!!!!!!98
    I2 (Internet 2r&t&c&l)!!!!!!!!!!99, 98, 9E, 9=
    I2$; (Internet 2r&t&c&l #ersi&n ;)!!!!!!!!!!9E
    S>T2 (Si ' /le >ail Transfer 2r&t&c&l)!!!!!!!!!!98
    TL2 (Trans ' issi&n L&ntr&l 2r&t&c&l)!!!!!!!!!!98, 9E
2r&GA!!!!!!!!!!E, 99, 9=
, estrisik&!!!!!!!!!!7, 9=
, isik&!!!!!!!!!!8, 7, <, 9;, 9=
Schad/r&gra ' ' !!!!!!!!!!8, =-95, 97
    Tr&3anisches 2ferd!!!!!!!!!!9<
    #irus!!!!!!!!!!97, 9<
    Wur ' !!!!!!!!!!9<
Schutzbedarf!!!!!!!!!!8, 9=
Sch) achstelle!!!!!!!!!!97
Sicherheits-Date) aA!!!!!!!!!!95, 9E, 9=
    LD (//licati&n-Le$el Date) aA)!!!!!!!!!!9=
    2aketfilter!!!!!!!!!!99, 9E, 9=
Sicherheitsleitlinie!!!!!!!!!!9=
Sicherheits ' aßnah ' e!!!!!!!!!!96, 9;, 9=
S>T2 (Si ' /le >ail Transfer 2r&t&c&l)!!!!!!!!!!98
S/a ' !!!!!!!!!!95, 9<
SAnc>L!!!!!!!!!!99, 9<
TL2 (Trans ' issi&n L&ntr&l 2r&t&c&l)!!!!!!!!!!98, 9E
TL21I2- , eferenz ' &dell!!!!!!!!!!
    *n) endungsschicht!!!!!!!!!!E, 98
    Internet-Schicht!!!!!!!!!!9E
    Trans/&rtschicht!!!!!!!!!!9E
Trans/&rtschicht!!!!!!!!!!9E
Tr&3anisches 2ferd!!!!!!!!!!9<
H>TS (Hni$ersal >&bile Telec& ' ' unicati&ns SAste ')!!!!!!!!!!8-E

#erf gbarkeit!!!!!!!!!!!!!!!!!!!!6, <, 97, 9<
#erschl sselung!!!!!!!!!!!!!!!!!!!!
Lhiffrat!!!!!!!!!!!!!!!!!!!!9<
#ertraulichkeit!!!!!!!!!!!!!!!!!!!!6, =, 96, 9E, 9<
#irenschutz!!!!!!!!!!!!!!!!!!!!94
#irenschutz/r&gra ' ' !!!!!!!!!!!!!!!!!!!!94, 9<
#irus!!!!!!!!!!!!!!!!!!!!94, 97, 9<
#&llzugriff!!!!!!!!!!!!!!!!!!!!7, 9<
#2N (#irtual 2ri$ate Net) &rk)!!!!!!!!!!!!!!!!!!!!8, E, <-96, 9<, 45
#2N-Date) aA!!!!!!!!!!!!!!!!!!!!E, 99-96, 45
Web-*n) endung!!!!!!!!!!!!!!!!!!!!=
WL*N (Wireless L&cal *rea Net) &rk)!!!!!!!!!!!!!!!!!!!!8, 7, <, 99, 45
Wur ' !!!!!!!!!!!!!!!!!!!!9<